9E0-100
(CSIDS)

Cisco Secure Intrusion Detection Systems

Version 6.0

www.testking.com

Leading The Way
in IT Testing And Certification Tools

www.testking.com

www.testking.com

Important Note, Please Read Carefully

Study Tips
This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

Further Material
For this test TestKing also provides Interactive Test Engine with Examinator.
Check out an Examinator Demo at http://www.testking.com/testking/index.cfm?pageid=724

Latest Version
We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check your member zone at TestKing an update 3-4 days before the scheduled exam date.

Here is the procedure to get the latest version:

1. Go to www.testking.com
2. Click on **Member zone/Log in**
3. The latest versions of all purchased products are downloadable from here. Just click the links.

For most updates, it is enough just to print the new questions at the end of the new version, not the whole document.

Feedback
Feedback on specific questions should be send to feedback@testking.com. You should state: Exam number and version, question number, and login ID.

Our experts will answer your mail promptly.

Copyright
Each pdf file contains a unique serial number associated with your particular name and contact information for security purposes. So if we find out that a particular pdf file is being distributed by you, TestKing reserves the right to take legal action against you according to the International Copyright Laws.

www.testking.com

Section A contains 80 questions. Section B contains 59 questions. The total number of questions is 139.

Section A

QUESTION NO: 1
If you wanted to list active telnet sessions and selectively end certain ones, what commands from the list below could you use on your PIX Firewall? (Choose all that apply)

A. show who
B. remove session
C. show logon
D. end session
E. kill
F. whois

Answer: A, E
Explanation:
Answer A. Show who: Shows active administrative Telnet sessions on the PIX Firewall. Cisco Secure Policy Manager does not generate this command, but the command can be supported using the Command panel on the PIX Firewall node. You can use the **who** command with the same results.
Answer E. kill: Terminates another Telnet session to PIX Firewall.

Reference: PIX Firewall Command Support Status

Incorrect Answers
B: remove session – is not a real command.
C: show logon – is not a real command.
D: end session – is not a real command.
F: whois – is a TCP literal name port (43 value)

QUESTION NO: 2
If you were using the ca authenticate command, you notice that it does not save to the PIX's configuration.
Is this normal or are you making a mistake?

A. The command is not saved to the config.
B. You need to Save Run-config-
C. It saves automatically, you need to retype it.
D. To see it you need to type show cert.

Answer: A
Explanation:

The **ca authenticate** command is not saved to the PIX Firewall configuration. However, the public keys embedded in the received CA (and RA) certificates are saved in the configuration as part of the RSA public key record (called the "RSA public key chain").

Reference: PIX Firewall Software Version 6.3 Commands

QUESTION NO: 3
Using the Cisco PIX and using port re-mapping, a single valid IP address can support source IP address translation for up to 64,000 active xlate objects.
This is an example of which technology?

A. PAT
B. DRE
C. SET
D. GRE
E. NAT

Answer: A
Explanation:
To allow all of the hosts access to the outside, we use Port Address Translation (PAT). If one address is specified in the **global** statement, that address is port translated. The PIX allows one port translation per interface and that translation supports up to 65,535 active xlate objects to the single global address. The first 1023 are reserved.

Reference: Cisco Secure PIX Firewall (Ciscopress) page 91
Using nat, global, static, conduit, and access-list Commands and Port Redirection on PIX

QUESTION NO: 4
With regards to the PIX Firewall, which two terms are correct from the below list?

A. All PIX Firewalls provide at least two interfaces, which by default, are called outside and inside.
B. All PIX Firewalls provide at least two interfaces, which by default, are called Eth1 and Eth2.
C. All PIX Firewalls provide at least two interfaces, which by default, are called Right and Left.
D. All PIX Firewalls provide at least two interfaces, which by default, are called Internet and External.

Answer: A
Explanation:
With a default configuration, Ethernet0 is named outside with a security level of 0 and Ethernet1 is named inside and assigned a security level of 100.

Reference: Cisco Secure PIX Firewall (Ciscopress) page 56

QUESTION NO: 5

What command could you use on your PIX Firewall to view the current names and security levels for each interface?

A. Show ifconfig
B. Show nameif
C. Show all
D. Ifconfig /all

Answer: B
Explanation:
Use the **show nameif** command to determine which interface is being described in a message containing this variable.

Reference: Cisco PIX Firewall Software Introduction

QUESTION NO: 6
Which TCP session reassembly configuration parameter enforces that a valid TCP session be establish before the Cisco IDS Sensor's sensing engine analyzes the traffic associated with the session?

A. TCP open establish timeout
B. TCP embryonic timeout
C. TCP closed timeout
D. TCP three way handshake
E. TCP sequence timeout

Answer: D
Explanation:
The goal of defining these reassembly settings is to ensure that the sensor does not allocate all of its resources to datagrams that cannot be completely reconstructed, either because the sensor missed some frame transmissions or because an attack is generating random fragmented datagrams.
To specify that the sensor track only sessions for which the three-way handshake is completed, select the **TCP Three Way Handshake** check box.

Reference: Tuning Sensor Configurations

QUESTION NO: 7
What can intrusion detection systems detect? (Choose three)

A. Network misuse
B. Network uptime
C. Unauthorized network access
D. Network downtime
E. Network throughput

F. Network abuse

Answer: A, C, F
Explanation:
An IDS is software and possibly hardware that detects attacks against your network. They detect intrusive activity that enters into your network. You can locate intrusive activity by examining network traffic, host logs, system calls, and other areas that signal an attack against your network.

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 54

QUESTION NO: 8
Which network device can be used to capture network traffic for intrusion detection systems without requiring additional configuration?

A. Hubs
B. Switches
C. Network taps
D. Router

Answer: A
Explanation: The ability to capture traffic may be inherent to a device technology or may require special features to provide this capability. For example, network hubs by their nature replicate data to all ports. Switches, on the other hand, rely on features such as port mirroring to permit the copy of specific traffic top another port.
Cisco Secure Intrusion Detection System 4 chap 5 page 3

QUESTION NO: 9
Which VLAN ACL sends only ftp traffic to a Cisco IDS Sensor connected to a Catalyst 6500 switch?

A. set security acl ip FTP_ACL permit udp any any eq 21
B. set security acl ipx FTP_ACL permit ip any any capture
C. set security acl ipx FTP_ACL permit tcp any any eq 21
D. set security acl ip FTP_ACL permit tcp any any eq 21 capture
E. set security acl ip FTP_ACL permit ip any any capture
F. set security acl ip FTP_ACL permit icmp any any eq 21

Answer: D
Explanation:
To create a VACL, you need to use the **set security acl ip** switch command. The syntax for capturing TCP traffic between a source IP address and a destination IP address is as follows:
set security acl *ip acl_name* **permit tcp** *src_ip_spec dest_ip_spec port* **capture**

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 505

Cisco Secure Intrusion Detection System 4 chap 5 page 33

QUESTION NO: 10
Which Cisco IDS communication infrastructure parameters are required to enable the use of IDS Device Manager to configure the Sensor? (Choose two)

A. Sensor organization name
B. Sensor group name
C. IDM group name
D. Sensor organization ID
E. IDM organization ID

Answer: A, D
Explanation:
Communication infrastructure parameters:
- Sensor Host ID and Organization ID
- Sensor Host Name and Organization Name
- Sensor IP Address
- Cisco Secure IDS Director or Cisco Secure PM IDS Manager Host ID and Organization ID
- Cisco Secure IDS Director or Cisco Secure PM IDS Manager Host Name and Organization Name
- Cisco Secure IDS Director or Cisco Secure PM IDS Manager workstation IP address

Reference: Cisco Secure Intrusion Detection System Sensor Configuration Note Version 2.5

QUESTION NO: 11
A company has purchased a Cisco IDS solution that includes IDS modules. The switch group had decided not to provide the security department interactive access to the switch. What IDSM feature should be configured to provide the security department access to the IDSM command line?

A. AAA
B. TFTP
C. HTTP
D. Telnet
E. HTTPS

Answer: D
Explanation:
The Catalyst 6000 family switch can be accessed either through a console management session or through telnet. Some switches might even support ssh access. After an interactive session is established with the switch, you must session into the ISDM line card. This is the only way to gain command-line access to the ISDM.

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 499

QUESTION NO: 12
Which network services are enabled by default on a Cisco IDS Sensor for remote management? (Choose three)

A. SSH
B. TFTP
C. SNMP
D. Telnet
E. RSH
F. FTP

Answer: A, D, F
Explanation:
Enter or delete the IP addresses of hosts and networks that can access the sensor via Telnet, FTP, SSH, and scp.

Reference: Cisco Intrusion Detection System Sensor Getting Started Version 3.1

Note by 2nd TestKing writer: I think the answers don't conform to the latest course manual.
Telnet – requires an IP address that has been assigned to the command and control interface via the CLI setup command. Must be enabled to allow telnet access. Telnet is DISABLED by default.
SSH – Requires an IP address that has been assigned to the command and control interface via the CLI setup command and uses a supported SSH client. The SSH server in the sensor is ENABLED by default.
HTTPS – Requires an IP address that has been assigned to the command and control interface via the CLI setup command and uses a supported web browser. HTTPS is ENABLED by default but can be disabled.
Cisco Secure Intrusion Detection System 4 chap 7 page 23

QUESTION NO: 13
When does the Sensor create a new log file?

A. Only when the Sensor is initially installed.
B. Only when the Sensor requests it.
C. Every time its services are restarted.
D. Every time a local log file is used.

Answer: C
Explanation:
The sensor creates new log file every time its services are restarted. This means that every time a new configuration is pushed to the sensor, a new configuration file is created
And the old file is closed and transferred to a temporary directory.

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 414

QUESTION NO: 14
Which Cisco IDSM partition must be active to install a signature update?

A. maintenance
B. root
C. /usr/nr
D. application
E. diagnostic

Answer: D
Explanation:
Make sure that the IDSM was booted in the application (hdd:1) and not the maintenance (hdd:2) partition. Use the switch command **show version** *module_number* to display the software version currently running on the module. The application partition will show a signature update version denoted by the letter "S" followed by a number, for example, 2.5(1)S1, but the maintenance partition will not contain the signature update version, for example 2.5(0).
Reference: Catalyst 6000 Intrusion Detection System Module Installation and Configuration Note Version 3.0(5)

QUESTION NO: 15
Which Cisco IDS software is included with a Sensor appliance?

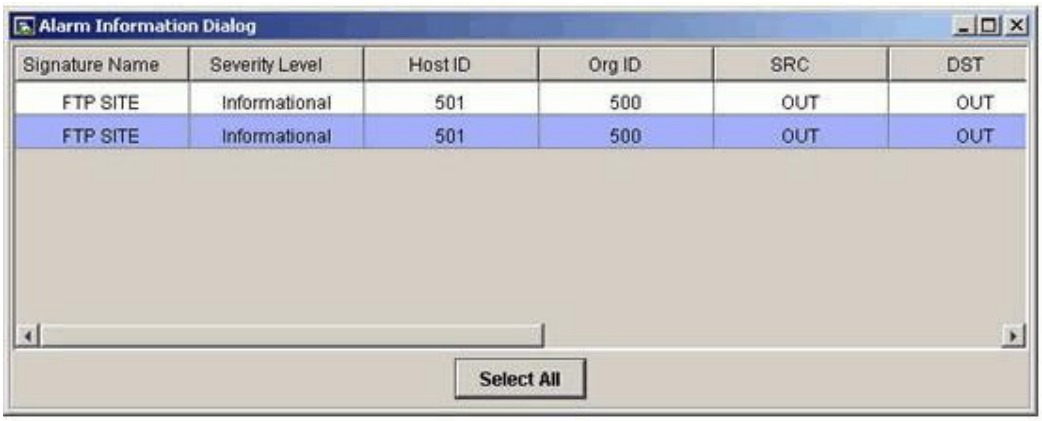
A. Cisco Secure Policy Manager
B. IDS Management Center
C. Intrusion Detection Director
D. IDS Event Viewer

Answer: D
Explanation: The IDS Event Viewer is a Java-based application that enables you to view and manage alarms for up to three sensors. With the IDS Event Viewer you can connect to and view alarms in real time or in imported log files. You can configure filters and views to help you manage the alarms. You can also import and export event data for further analysis. The IDS Event Viewer also provides access to the Network Security Database (NSDB) for signature descriptions.

Reference: Cisco Intrusion Detection System Event Viewer Version 3.1

Note by 2nd TestKing writer:
I am not sure about this question. The latest course manual 4, states that the IDM "is a web-based, embedded architecture configuration tool for cisco ids sensors." Cisco Secure Intrusion Detection System 4 chap 10 page 4

QUESTION NO: 16
Exhibit:



In the Cisco IDS Event Viewer, how do you display the context data associated with an event?

A. Choose **View>Context Data** from the main menu.
B. Right-click the event and choose **Show Data**.
C. Choose **View>Show** data from the main menu.
D. Right-click the event and choose **Show Context**.
E. Choose **View>Show Context** from the main menu.
F. Double-click the event.

Answer: D
Explanation:
Certain alarms may have context data associated with them. Context data provides a snapshot of the incoming and outgoing binary TCP traffic (up to a maximum of 256-bytes in both directions) that preceded the triggering of the signature. To view the context for an alarm, follow these steps:
Step 1 From the Alarm Information Dialog, right-click a cell in the Context column, and then select **Show Context**.
Step 2 Scroll to view the context associated with this alarm.

Reference: Cisco Intrusion Detection System Event Viewer Version 3.1
Also see Cisco Secure Intrusion Detection System 4 chap 10 page 20

QUESTION NO: 17
When designing IP blocking, why should you consider entry points?

A. They provide different avenues for the attacker to attack your networks.
B. They prevent all denial of service attacks.
C. They are considered critical hosts and should not be blocked.
D. They provide a method for the Sensor to route through the subnet to the managed router.

Answer: A
Explanation:

Today's networks have several entry points to provide reliability, redundancy, and resilience. These entry points also represent different avenues for the attacker to attack your network. You must identify all the entry points into your network and decide whether they need to also participate in IP blocking.

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 467
Cisco Secure Intrusion Detection System 4 chap 15 page 8

Note: It is recommended that Sensors be placed at those network entry and exit points that provide sufficient intrusion detection coverage. Cisco Secure Intrusion Detection System 4 chap 4 page 37

QUESTION NO: 18
Which type of ACL is allowed when implementing the Cisco IDS IP blocking feature pre-shun ACLs?

A. Named IP extended
B. Named IP standard
C. Numbered IPX standard
D. Numbered IPX extended
E. Named IPX extended

Answer: A
Explanation: A pre-block and post-block ACL must be an extended IP ACL, named or unnumbered. They should be configured on the device Sensor block is configured for that interface/direction Cisco Secure Intrusion Detection System 4 chap 15 page 15

QUESTION NO: 19
Which of the following commands let you view, change, enable, or disable the use of a service or protocol through the PIX Firewall?

A. fixing protocol
B. set firewall
C. fixup protocol
D. change –all fix

Answer: C
Explanation:
The **fixup protocol** commands let you view, change, enable, or disable the use of a service or protocol through the PIX Firewall. The ports you specify are those that the PIX Firewall listens at for each respective service.

Reference: Cisco PIX Firewall Command Reference, Version 6.3
Note: In Appendix B of the Cisco Secure Intrusion Detection System 4 Fixup protocol is not talked about.

QUESTION NO: 20
Debugging a PIX is what you want to do to resolve a problem.
What command would you use to display the current state of tracing?

A. show debug
B. debug all
C. all on debug
D. debug crypto

Answer: A
Explanation:
The **debug** command lets you view debug information. The **show debug** command displays the current state of tracing. You can debug the contents of network layer protocol packets with the **debug packet** command

Reference: Cisco PIX Firewall Command Reference, Version 6.3
. **Note**: in Appendix B of the Cisco Secure Intrusion Detection System 4 Debugging is not talked about.

QUESTION NO: 21
RIP uses a port to establish communications. If you were to block it with your Firewall, what port would you be concerned about?

A. Port 345
B. Port 345
C. Port 520
D. Port 354

Answer: C
Explanation:
Port 520 is the Routing Information Protocol port.

Reference: Cisco PIX Firewall Software - Introduction
Note: Rip is not talked about in this manner in the course manual 4

QUESTION NO: 22
Exhibit:

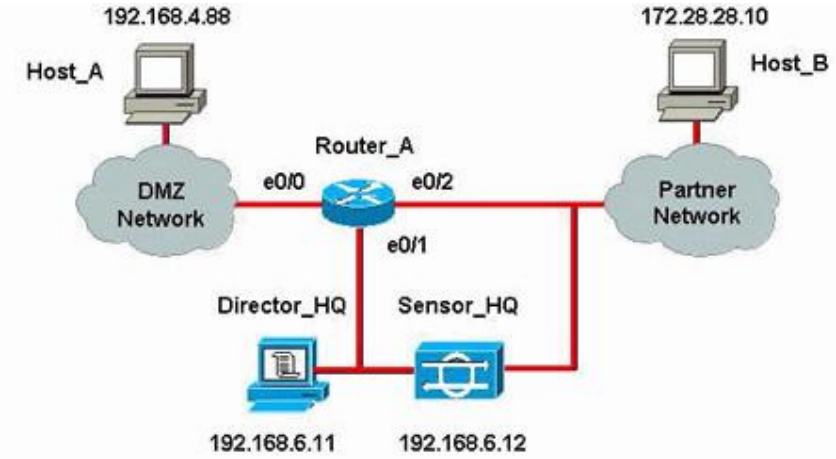
If you were looking at the back of your PIX firewall and saw the following plate, what model of PIX would you be working on?

A. 501
B. 506
C. 515

D. 1100

Answer: C
Reference: Cisco Secure PIX Firewall

QUESTION NO: 23
Exhibit:



The company has decided to block using the interface connected to the Internet; the Sensor must communicate only with devices on the same network.
Which Cisco IOS router interface should the sensor use to establish an interactive session that implements blocking?

A. e0/2
B. e0/0
C. e1/0
D. e0/1
E. e1/1

Answer: D
The Sensor is on the same network, so that means the only possibly answer is the Ethernet01 interface. Ethernet0/2 is using a different network address and Ethernet0/0 is using a DMZ network.

Note: What is being talked about here is a Network Tap. " A network tap is a device used to split full-duplex traffic flows into a single traffic flows that can be aggregated at a switch device. The network tap has four connectors
Two input connectors – traffic from a device
Two output connectors- traffic exiting the tap"
Cisco Secure Intrusion Detection System 4 chap 5 page 7

QUESTION NO: 24

An ACL policy violation signature has been created on a Cisco IDS Sensor. The Sensor is configured to receive policy violations from a Cisco IOS router.
What configurations must exist on the router? (Choose two)

A. Logs permit ACL entries
B. Logs deny ACL entries
C. Sends SNMP traps to the Sensor
D. Sends Syslog messages to the Sensor
E. Sends SNMP traps to the Director
F. Sends syslog messages to the Director

Answer: B, F
Explanation:
The Sensor can be configured to create an alarm when it detects a policy violation from the syslog generated by a Cisco router. A policy violation is generated by a Cisco router when a packet fails to pass a designated Access Control List. Security data from Sensor and Cisco routers, including policy violations, is monitored and maintained on the Director.

Reference: Cisco Secure Intrusion Detection System Overview

QUESTION NO: 25
A Cisco IDS Sensor has been configured to detect attempts to extract the password file from Windows 2000 systems. During a security posture assessment, the consultants attempted to extract the password files from three Windows 2000 servers.
This activity was detected by the Sensor.
What situation has this activity caused?

A. True negative
B. True positive
C. False negative
D. False positive

Answer: B
Explanation:
True positive – is when an IDS generates an alarm for known intrusive activity.
False negative – is when an IDS fails to generates an alarm for known intrusive activity.
False positive - is when an IDS generates an alarm for normal user activity.

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 55 & 58

Note: True positive –A situation in which a signature is fired properly when offending traffic is detected. An attack is detected as expected. - Cisco Secure Intrusion Detection System 4 chap 3 page 12

QUESTION NO: 26

What Cisco IDS Sensor secure shell operation enables a network security administrator to remove hosts from the list of those previously connected to devices?

A. Generate new Sensor SSH keys.
B. Generate new Director SSH keys.
C. Manage the Sensor's known hosts file.
D. Manage the Director's known hosts file.

Answer: C
Explanation: Access to the probe is determined by a ACL but note in chap 12 the MC deals with SSH key generation.
Sensor#config t
Sensor#(Config)#service host
Sensor#(config-host)networkParams
Sensor#(config-host-net) accesslist ip address 10.0.2.0 netmask 255.255.255.0 ----adds an entire network to the access list
Cisco Secure Intrusion Detection System 4 chap 9 page 31

QUESTION NO: 27
Which user account is used to log into the IDSM?

A. Root
B. Administrator
C. Netranger
D. Ciscoidsm
E. Ciscoids

Answer: E
Explanation:
The default user login user name for the Cisco IDS Module is Ciscoids, and the default password is attack.

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 680

Note: This was correct in the older course however it is not right according to 4 but the answers given don't match what is listed in the course manual.
"Log in to the IDSM2 using the default username CISCO and the Password CISCO" - Cisco Secure Intrusion Detection System 4 chap 8 page 12

"The sensor allows you to create multiple local user accounts. The default username and password is cisco. You are required to change the default password the first time you log on." - Cisco Secure Intrusion Detection System 4 chap 7 page 24

QUESTION NO: 28

Which Cisco IDS software update file can be installed on a IDS-4210 Sensor?

A. IDSMk9-sp-3.0-3-S10.exe
B. IDSMk9-sp-3.0-3-S10.bin
C. IDSMk9-sig-3.0-3-S10.exe
D. IDSk9-sp-3.1-2-S24.exe
E. IDSk9-sp-3.1-2-S24.bin
F. IDSk9-sig-3.1-2-S24.exe

Answer: E
Explanation: D is not the correct answer. I have an example in the course guide 4 that show the.bin is correct. Also supported in appendix C-17 (bin-this is the executable files directory. It includes all of the cisco IDS services, programs, and functions)
IDS-k9-sp-4.0-2-s42.rpm.pkg - executable file that contains signature or service pack update. This is not an option but it is shown on 17-8
Sensor(config)#upgrade
ftp://cisco@192.168.1.1/ids-k9-sp4.0-2-s29.bin - Installs the IDS-k9-sp-4.0-2-s29.bin from the ftp server's root directory at IP address 192.168.1.1 with user name of cisco
- Cisco Secure Intrusion Detection System 4 chap 17 page 10

QUESTION NO: 29
Exhibit:

```
netrangr@sensor1:/usr/nr
$idsstatus
netrangr 16249     1  0 15:46:33 pts/1    0:00 /usr/nr/bin/nr.postofficed
netrangr 16267     1  0 15:46:34 pts/1    0:00 /usr/nr/bin/nr.sapd
netrangr 16295     1  0 15:46:35 pts/1    0:00 /usr/nr/bin/nr.managed
netrangr 16258     1  0 15:46:34 pts/1    0:00 /usr/nr/bin/nr.loggerd
netrangr 16274     1  0 15:46:34 pts/1    0:00 /usr/nr/bin/nr.fileXferd
netrangr 16282     1 18 15:46:34 pts/1    0:08 /usr/nr/bin/nr.packetd
```

Given the output of the idsstatus Sensor command. What function is the Sensor performing? (Choose two)

A. Not logging alarms, commands, and errors.
B. Performing IP blocking.
C. Not capturing network traffic.
D. Logging alarms, commands, and errors.
E. Not performing IP blocking.

Answer: B, D
Explanation:
Postofficed The *postofficed* daemon serves as the communication vehicle for the entire Cisco IDS product
Sapd - The *sapd* daemon is a user-configurable scheduler that controls database loading and archival of old event and IP session logs.
Managed - The *managed* daemon is responsible for managing and monitoring network devices (routers and packet filters). For example, when *packetd* identifies that a certain type of attack should be shunned, it sends a shun command to *managed* via the post office facility.

Loggered The *loggerd* daemon writes out sensor and error data to flat files generated by one or more of the other daemons.
fileXferd The *fileXferd* daemon is used for file transfer between Sensors and Directors. It is used to transport configuration files between Directors and Sensors.
Packetd - The *packetd* daemon interprets and responds to all of the events it detects on the monitored subnet.

Reference: Cisco Secure IDS Internal Architecture

QUESTION NO: 30
What is the Cisco IDS Management Center?

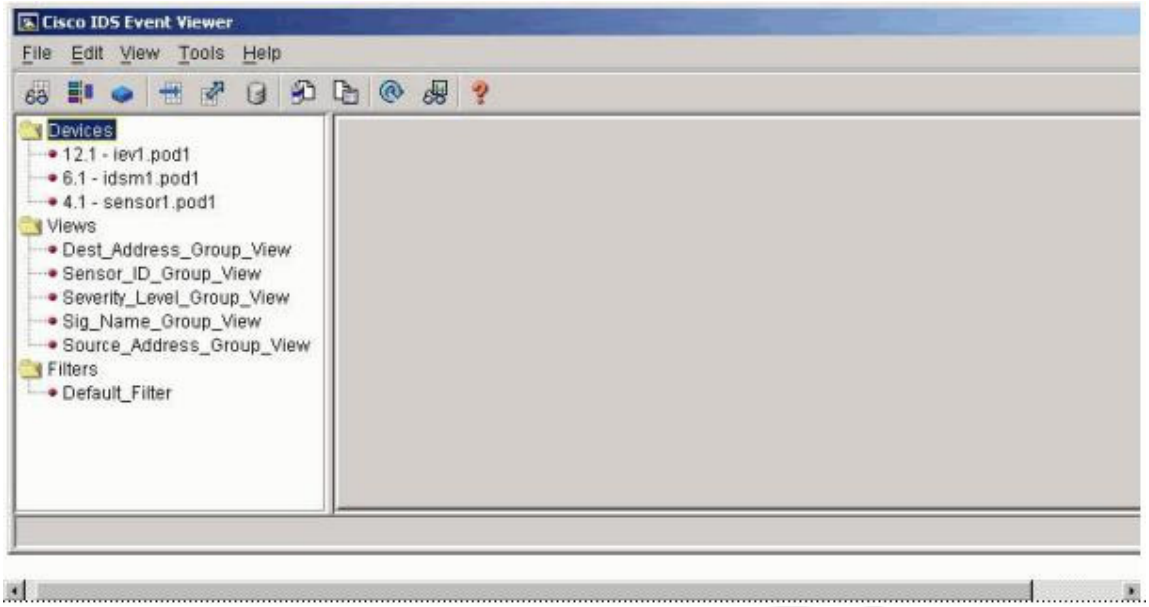
A. Web-based interface for managing and configuring multiple sensors.
B. Command-line interface for managing and configuring multiple sensors.
C. Web-based interface for managing and configuring a single sensor.
D. Command-line interface for managing and configuring a single sensor.

Answer: A
Explanation:
The Management Center for IDS Sensors is a tool with a scalable architecture for configuring Cisco network sensors, switch IDS sensors, and IDS network modules for routers. Uses a web-based interface.

Reference: CiscoWorks Management Center for IDS Sensors Datasheet

Note: What is the IDS MC? The IDS MC is a web-based application that centralizes and accelerates the deployment and management of multiple IUDS sensors of IDSM. IDS MC is a component of the VMS bundle. - Cisco Secure Intrusion Detection System 4 chap 11 page 3

QUESTION NO: 31
Exhibit:



After 1EV has been configured to receive alarms from Sensors, how do you display the alarms in the Cisco IDS Event Viewer? (Choose all that apply)

A. Right-click **Dest_Address_Group_View** and choose **View**.
B. Double-click **Dest_Address_Group_View**
C. Right-click **Dest_Address_Group_View** and choose **Display**.
D. Right-click **Sig_Name_Group_View** and choose **View**.
E. Right-click **Sig_Name_Group_View** and choose **Display**.
F. Double-click **Sig_Name_Group_View**

Answer: B, F
Explanation:
Right-click a row in the Expanded Details Dialog, and then select View Alarms.
Result: The Alarm Information Dialog appears.
-or-
Double-click the cell containing the alarms you want to view in the Total Alarm Count column. Result: The Alarm Information Dialog appears.

Reference: **Cisco IDS Sensor Software - Cisco Intrusion Detection System Event Viewer Version 3.1**

Note: To view the alarm information, right-click the alarm in the Expanded Details Dialog window and choose View Alarms. The alarm Information Dialog window displays each event and the associated alarm data, such as Signature Name, Source address, and Destination address. - Cisco Secure Intrusion Detection System 4 chap 10 page 19

QUESTION NO: 32

Which Cisco IDS Sensor configuration parameter affects the source and destination values included in an IDS alarm event?

A. Data source
B. IP fragment reassembly
C. External network definition
D. Internal network definition
E. TCP reassembly
F. Sensor IP address

Answer: D
Explanation:
You can use the source and destination location to alter your response to specific alarms. Traffic coming from a system within your network to another internal host that generates an alarm may be acceptable, whereas, you might consider this same traffic, originating from an external host or the Internet, totally unacceptable.

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 183

QUESTION NO: 33
Which TCP session reassembly configuration parameter enforces that a valid TCP session be establish before the Cisco IDS Sensor's sensing engine analyzes the traffic associated with the session?

A. TCP open establish timeout
B. TCP embryonic timeout
C. TCP closed timeout
D. TCP three way handshake
E. TCP sequence timeout

Answer: D
Explanation:
Select the TCP three way handshake if you want the sensor to tack only those sessions for which the three-way handshake is completed. The other options for reassembly are:
No reassembly
Loose reassembly
Strict reassembly

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 419

QUESTION NO: 34
Which common command are you going to use to clear the contents of the translation slots when needed?

A. clear xlate
B. clear translate
C. clear all

D. show translate

Answer: A
Explanation:
The **xlate** command allows you to show or clear the contents of the translation (xlate) slots.
show xlate, clear xlate

Reference: Cisco Secure PIX Firewall (Ciscopress) page 77

QUESTION NO: 35
When working on your PIX, you would like to view the network states of local hosts. What command could you use?

A. local host all
B. show local-host
C. show host all
D. show local remote
E. show set local

Answer: B
Explanation:
The **show local-host** command assists you in characterizing your "normal" load on a statically translated host, both before and after setting limits.

Reference: Cisco Secure PIX Firewall (Ciscopress) page 171

QUESTION NO: 36
If you wanted to enable access to a higher security level interface from a lower level interface what could you do?

A. Set the conduit to 0/1.
B. Use the static and access-list commands.
C. Set the Eth1/0 interface to auto.
D. Use the nat and global commands.

Answer: B
Explanation:
Two things are required for traffic to flow from a lower security to a higher security interface: a static translation and a conduit or an access list to permit the desired traffic.

Reference: Cisco Secure PIX Firewall (Ciscopress) page 55

QUESTION NO: 37
A company has a requirement to create a custom signature that detects BGP packets traversing the network.
Which Cisco IDS signature micro-engine can be used to create this signature?

A. Atomic.TCP
B. Atomic.L3.IP
C. Sweep.Port.TCP
D. Atomic.IPOptions

Answer: B
Explanation:
The following are Atomic.l3.IP parameters:
MaxProto-defines the maximum IP protocol number, after which the signature fires
MinProto-Defines the minimum IP protocol number, after which the signature fires
isRFC1918-Defines whether the packet is from RFC 1918 address pool
-Cisco Secure Intrusion Detection System 4 chap 13 page 13

BGP is a layer 3 routing protocol. Atomic.L3.IP will detect layer 3 IP alarms

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 628

QUESTION NO: 38
A Cisco IDS Sensor has been configured to detect attempts to extract the password file from Windows 2000 systems. During a security assessment, the consultants attempted to extract the password files from three Windows 2000 servers. This activity was not detected by the Sensor.
What situation has this activity caused?

A. False negative
B. False positive
C. True positive
D. True negative

Answer: A
False negative – is when an IDS fails to generates an alarm for known intrusive activity.
False positive - is when an IDS generates an alarm for normal user activity.
True positive – is when an IDS generates an alarm for known intrusive activity.

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 55 & 58

Note: A situation in which a signature is not fired when offending traffic is detected. An actual attack is not detected -Cisco Secure Intrusion Detection System 4 chap 3 page 11

QUESTION NO: 39
A company has installed an IDSM into a Catalyst 6509 switch in slot 9. The network security architect has designed a solution that requires the IDSM monitor traffic only from VLAN 199.
Which Catalyst OS commands are used to achieve this configuration?

A. set trunk 9/2 199
B. clear trunk 9/2 199

C. clear trunk 9/2 1-1024
D. clear trunk 9/1 1-1024
E. set trunk 9/1 199
F. clear trunk 9/1 199

Answer: D, E
Reference: **Cisco Catalyst 5000 Series Switches - Switch and ROM Monitor Commands¿Release 6.2**

Note: In the new course we think the answer would be this
Router(config)#interface vlan <vlan_number> - creates or access the vlan interface specified
Router(config)# interface vlan 401
Router(config-if)mlp ip ids <acl_name> - applies an IP acl to the vlan interface
The mpl ip ids command is used to apply an extended ip access list to the vlan interface
-Cisco Secure Intrusion Detection System 4 chap 5 page 48

QUESTION NO: 40
How many interactive login sessions to the IDSM are allowed?

A. 1
B. 2
C. 3
D. 4

Answer: A
Note: In the IDSM chapter I did not come across anything that stated this. In fact there is not much listed in the IDSM chapter. The main thrust was that it uses the same code as the ver4 sensors so it works the same except for some alterations.. Cisco Secure Intrusion Detection System 4 chap 4

QUESTION NO: 41
The Cisco IDS Sensor service pack file IDSk9-sp-3.1-2-S23.bin exists on the Sensor. Which command installs the service pack on the Sensor?

A. IDSk9-sp-3.1-2-S23 –install
B. IDSk9-sp-3.1-2-S23.bin –install
C. IDSk9-sp-3.1-2-S23.bin –i
D. IDSk9-sp-3.1-2-S23.bin –l
E. IDSk9-sp-3.1-2-S23-bin –apply
F. IDSk9-sp-3.1-2-S23 –apply

Answer: E

Explanation:
Valid Service Pack upgrade
idsm(config)# apply ftp://user@10.0.0.1//IDSMk9-sp-3.0-3-S10.exe

Reference: Cisco Intrusion Detection System - Upgrading the Intrusion Detection System Module

I am not sure about answer D. I really cant find anything that supports it. In the new course the command is update. I think that the answer may be E using the apply command as shown in the explanation.

QUESTION NO: 42
Which network management product is used to deploy configurations to groups of IDS devices?

A. IDM
B. IDS Management Center
C. Security Monitoring
D. IEV

Answer: B
Explanation:
The Management Center for IDS Sensors is a tool with a scalable architecture for configuring Cisco network sensors, switch IDS sensors, and IDS network modules for routers. Uses a web-based interface.

Reference: CiscoWorks Management Center for IDS Sensors

QUESTION NO: 43
A hospital's security policy states that any e-mail messages with the words SSN or Social Security must be detected by the IDS Sensor.
Which Cisco IDS signature micro-engine should be used to create the signature?

A. Atomic.TCP
B. Atomic.UDP
C. String.ICMP
D. String.TCP
E. String.UDP

Answer: E (or D)
Note: I am not sure why the original person who answered this question picked tcp but I think that most email is delivered via tcp. However he/she is correct in that it is a string signature. Off hand I have a slight doubt if most email is delivered via UDP or TCP. If you think that most email is UDP pick E if you don't then stay with the given answer.
ICMP is wrong.
Atomic is one packet and wrong.
The course manual does not give examples of String signatures.

Cisco Secure Intrusion Detection System 4 chap 13 page 41

QUESTION NO: 44
What information can a network security administrator specify in a Cisco IDS exclude signature filter? (Choose two)

A. Signature name
B. Signature ID
C. Signature action
D. Signature severity level
E. Sub-signature ID
F. Source port

Answer: B, E
Explanation:
When defining a simple filter, you need to configure the following fields:
- Signature
- Subsignature
- IP address
- Network Mask
- Address Role

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 446

QUESTION NO: 45
Which common command are you going to use to clear the contents of the translation slots when needed?

A. clear xlate
B. remove session
C. show logon
D. end session
E. kill
F. whois

Answer: A
The **xlate** command allows you to show or clear the contents of the translation (xlate) slots.
show xlate, clear xlate

Reference: Cisco Secure PIX Firewall (Ciscopress) page 77

QUESTION NO: 46
If you wanted to view the conduit command statements in the configuration and the number of times (hit count) an element has been matched during a conduit command search, what command would you type on the PIX Firewall?

A. show con –all
B. show config
C. show conduit
D. conduit /all

Answer: C
Explanation:
To look at the configured conduits, use the show conduit command.

Reference: Cisco Secure PIX Firewall (Ciscopress) page 89

QUESTION NO: 47
In PIX Terminology, what exactly is a Conduit?

A. It routes data from one interface to another.
B. The Conduit is where the data travels on the Bus.
C. It controls what QoS the packets get when going through Eth1.
D. Controls connections between external and internal networks.

Answer: D
Explanation:
the **conduit** command functions by creating an exception to the PIX Firewall Adaptive Security Algorithm that then permits connections from one PIX Firewall network interface to access hosts on another.
Reference: Cisco PIX Firewall Command Reference, Version 6.3

QUESTION NO: 48
Which value can be assigned to define the Cisco IDS 4210 Sensor's sensing interface?

A. Auto
B. Detect
C. Probe
D. Sniffing
E. Select

Answer: D
Explanation:
An individual sensor contains two separate interfaces. The sensor used on of the interfaces to passively sniff all the network packets by placing the interface in Promiscuous mode. The sensor uses the other network interface for command and control traffic.
Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 98

QUESTION NO: 49

The network administrator has informed the security administrator that the average number of packets per seconds is 400.
Which Sensor selection factor should the security administrator take into consideration?

A. Sensor processor speed
B. Server performance
C. Network throughput
D. Intrusion detection analysis performance.

Answer: D
Explanation:
Real-time monitoring of network packets, which involves packet capture and analysis

Reference: **Cisco IDS Sensor Software - Cisco Secure Intrusion Detection System Overview**

QUESTION NO: 50
Which Cisco IDS communication infrastructure parameters are required to enable the use of the IDS Device Manager to configure the Sensor? (Choose two)

A. IEV IP address
B. Sensor IP address
C. IDM IP address
D. Sensor host name
E. IEV host name
F. IDM host name

Answer: B, D

Communication infrastructure parameters:
- Sensor Host ID and Organization ID
- Sensor Host Name and Organization Name
- Sensor IP Address
- Cisco Secure IDS Director or Cisco Secure PM IDS Manager Host ID and Organization ID
- Cisco Secure IDS Director or Cisco Secure PM IDS Manager Host Name and Organization Name
- Cisco Secure IDS Director or Cisco Secure PM IDS Manager workstation IP address

Reference: Cisco Secure Intrusion Detection System Sensor Configuration Note Version 2.5

QUESTION NO: 51
Which management access methods require that an IP address be assigned to a Cisco IDS Sensor? (Choose three)

A. IDS Device Manager
B. IDS Event Viewer
C. Remote Shell
D. Secure Shell
E. Telnet
F. Trivial File Transfer Protocol

Answer: A, D, E
Explanation:
Enter or delete the IP addresses of hosts and networks that can access the sensor via Telnet, FTP, SSH, and scp.

Reference: Cisco Intrusion Detection System Sensor Getting Started Version 3.1

QUESTION NO: 52
Exhibit:

```
netrangr@sensor1:/usr/nr
$idsstatus
netrangr 16249     1  0 15:46:33 pts/1    0:00 /usr/nr/bin/nr.postofficed
netrangr 16267     1  0 15:46:34 pts/1    0:00 /usr/nr/bin/nr.sapd
netrangr 16295     1  0 15:46:35 pts/1    0:00 /usr/nr/bin/nr.managed
netrangr 16258     1  0 15:46:34 pts/1    0:00 /usr/nr/bin/nr.loggerd
netrangr 16274     1  0 15:46:34 pts/1    0:00 /usr/nr/bin/nr.fileXferd
netrangr 16282     1 18 15:46:34 pts/1    0:08 /usr/nr/bin/nr.packetd
```

Given the output of the idsstatus Sensor command, what function is the Sensor performing?

A. Capturing network traffic.
B. Not performing IP blocking.
C. Not logging alarms, errors, and commands.
D. Generating e-mails for alarms.
E. Not capturing network traffic.
F. Loading alarms into a user database.

Answer: A
Explanation:
Postofficed The *postofficed* daemon serves as the communication vehicle for the entire Cisco IDS product
Sapd - The *sapd* daemon is a user-configurable scheduler that controls database loading and archival of old event and IP session logs.
Managed - The *managed* daemon is responsible for managing and monitoring network devices (routers and packet filters). For example, when *packetd* identifies that a certain type of attack should be shunned, it sends a shun command to *managed* via the post office facility.
Loggered The *loggerd* daemon writes out sensor and error data to flat files generated by one or more of the other daemons.
fileXferd The *fileXferd* daemon is used for file transfer between Sensors and Directors. It is used to transport configuration files between Directors and Sensors.
Packetd - The *packetd* daemon interprets and responds to all of the events it detects on the monitored subnet.

Reference: Cisco Secure IDS Internal Architecture

QUESTION NO: 53
What Cisco IDS software is included with a Sensor appliance? (Choose two)

A. IDS Management Center
B. IDS Device Manager
C. Intrusion Detection Director
D. Cisco Secure Policy Manager
E. IDS Event Viewer

Answer: B, E
Explanation: The Cisco IDS Device Manager and IDS Event Viewer, both delivered through Cisco IDS software version 3.1, are part of Cisco's multi-tiered management strategy addressing the administrative needs of e-business security. The IDS Device Manager enables easy, remote IDS sensor configuration with a high degree of customization, minimizing the occurrence of false positives. The event monitoring capabilities delivered via the IDS Event Viewer let customers collect, correlate, and analyze event data for rapid detection and response to unauthorized network activity.

Reference: Cisco Addresses Intrusion Protection with new IDS Solutions

QUESTION NO: 54
A Cisco IDS Sensor is capturing large volumes of network traffic. Which Cisco IDS Sensor status alarm is an indication that the Sensor is being overwhelmed?

A. Daemon down
B. Route down
C. No traffic
D. Captured packet count
E. Missed packet count
F. Network saturated

Answer: E
Explanation: Problem: sensorApp does not respond after hours of being seriously oversubscribed. All system memory, including SWAP, is exhausted when a 700 Mbps traffic feed is sent to the 250 Mbps appliance 4235 over several hours.

Symptom: The CLI show version command may say "AnalysisEngine Not Running" or control transactions will timeout with error about sensorApp not responding. You will see 993 missed packet alarms before the unresponsive state (if that alarm is Enabled).

Workaround: 1) Do not seriously oversubscribe the sensor. Chose the right appliance for your network segment and partition the traffic accordingly. 2) If sensorApp (aka AnalysisEngine) is listed as Not Running or is not responsive, issue a RESET command on the CLI. Do this

after examining the traffic feed and adjusting the feed to the sensor so it is within the rating for the specific appliance
http://www.cisco.com/en/US/partner/products/sw/secursw/ps2113/prod_release_note09186a00801a00ac.html

QUESTION NO: 55
Which PIX Command will allow the PIX Firewall to authenticate its certification authority (CA) by obtaining the CA's self-signed certificate, which contains the CA's public key?

A. ca lock /all
B. show auth
C. Set ca auth
D. ca authenticate

Answer: D
Explanation: The **ca authenticate** command allows the PIX Firewall to authenticate its certification authority (CA) by obtaining the CA's self-signed certificate, which contains the CA's public key.

Reference: Cisco PIX Firewall Command Reference, Version 6.3

QUESTION NO: 56
What port would you be concerned about if you were worried bout DNS Zone Transfers while protecting your infrastructure with a PIX?

A. UDP 12
B. UDP 53
C. TCP 62
D. UDP 45

Answer: B
Explanation:
Triggers on normal DNS zone transfers, in which the source port is 53.

Reference: Cisco IOS Intrusion Detection System Signature List

QUESTION NO: 57
If you wanted to show the running configuration of a PIX firewall, what command would you use?

A. Show Running-Config
B. Write terminal
C. Show Config
D. Show pix

Answer: B
Explanation:
Write terminal displays current configuration on the terminal.

Reference: Cisco PIX Firewall Command Reference, Version 6.3

QUESTION NO: 58
Which Cisco IDS signatures are affected by the Sensor's level of traffic logging value?

A. String signatures
B. HTTP signatures
C. TCP connection signatures
D. FTP connection signatures
E. ICMP signatures

Answer: C
Explanation:
Connection signatures are user-configurable attack signatures based on the transport-layer protocol (TCP or UDP) and port number of the packets being monitored
Reference: Sensor Signatures

QUESTION NO: 59
An anonymous person has posted a tool on a public website that can cause Cisco DSL routers to reboot.
What term describes how this tool is used to leverage the weakness in the Cisco DSL routers?

A. Vulnerability
B. Exploit
C. Rootkit
D. Exposure

Answer: B
Explanation:
Exploits activity—Indicative of someone attempting to gain access or compromise systems on your network, such as Back Orifice, failed login attempts, and TCP hijacking

Reference: Cisco Intrusion Detection System - Cisco Secure Intrusion Detection System

QUESTION NO: 60
A university's security policy states that network devices must be managed using secure communication methods.
Which Cisco IDS Sensor services must be disabled to meet this requirement? (Choose two)

A. SSH

B. Telnet
C. TFTP
D. SNMP
E. FTP
F. RSH

Answer: B, E
Explanation: The Sensor always provides secure shell services (including scp). Increase the security of the Sensor by disabling two services that allow clear text password authentication: Telnet and FTP. For maximum security disable both.

Reference: Cisco IDS Sensor Software - Cisco Intrusion Detection System Sensor Configuration Note Version 3.1

QUESTION NO: 61
A company policy states that IDS Sensors can be managed only by authorized management workstations. The management workstations exist on the 192.168.21.0/24 network.
Which address must the network security administrator add to the Cisco IDS Sensor's network access control list?

A. 192.168.21.
B. 192.168.21
C. 192.168.
D. 192.168
E. 192.168.21.0.
F. 192.168.21.0

Answer: F
Explanation: I am not sure the difference between E and F except for an extra dot (which is wrong)
Actually the original answer is A 192.168.21. which is wrong as far as version 4 of the course manual is concerned. I think this answer was wrong. Acls you must put all aspects of the 4 octets in. I think the correct was the 192.168.21.0 the original had 192.168.21. - nothing in the fourth octet
Sensor#config t
Sensor(config)# service host
Sensor(config-Host)#netwrokParams
Sensor(config-Host-net) accesslist ipAddress 10.0.2.0 netmask 255.255.255.0 - adds an entire network to the access list.
Cisco Secure Intrusion Detection System 4 chap 13 page 41

QUESTION NO: 62
A Cisco IDS Sensor has been configured to perform IP Blocking.
Which Cisco IDS service must be running on the Sensor?

A. Logged
B. Eventd
C. Blocked
D. Managed
E. Shunned

Answer: D
Explanation:
Managed - The *managed* daemon is responsible for managing and monitoring network devices (routers and packet filters). For example, when *packetd* identifies that a certain type of attack should be shunned, it sends a shun command to *managed* via the post office facility.

Reference: Cisco Secure IDS Internal Architecture

QUESTION NO: 63
In the Cisco IDS Management Center, what workflow steps must you perform to push configuration files to a Sensor?

A. Configure, load, submit
B. Generate, approve, deploy
C. Generate, submit, approve
D. Load, submit, approve

Answer: B
Explanation:
The Workflow tab is where you can generate, approve, and deploy configuration files for the sensors that you want to manage with your installation of IDS MC

Reference: Generating, Approving, and Deploying Configuration Files

QUESTION NO: 64
A company has a custom client-server application that communicates on UDP ports 6000-7000.
Which Cisco IDS signature micro-engine can be used to detect attempts to locate the servers?

A. Atomic.IPOptions
B. Sweep.RPC
C. Sweep.Net.UDP
D. Sweep.Port.UDP
E. String.Net.UDP
F. String.Port.UDP

Answer: D
Explanation:
SWEEP.PORT.UDP - UDP connections to multiple destination ports between two nodes

Reference: Cisco Secure Intrusion Detection System Signature Engines Version 3.0

QUESTION NO: 65
Which command(s) from the list below generates RSA key pairs for your PIX Firewall?

A. rsa set ca
B. ca generate rsa
C. ca rsa config
D. config rsa

Answer: B
Explanation:
The **ca generate rsa** command generates RSA key pairs for your PIX Firewall. RSA keys are generated in pairs—one public RSA key and one private RSA key

Reference: Cisco PIX Firewall Command Reference, Version 6.3

QUESTION NO: 66
Cisco PIX will support which protocols listed below?

A. PIX Supports all listed here.
B. File Transfer Protocol (FTP)
C. Domain Name System (DNS)
D. Bootstrap Protocol (BOOTP)
E. Generic Route Encapsulation (GRE)

Answer: A
Explanation:
Supported Protocols and Applications
PIX Firewall supports the following TCP/IP protocols and applications:

- Address Resolution Protocol (ARP)
- Archie
- Berkeley Standard Distribution (BSD)-rcmds
- **Bootstrap Protocol (BOOTP)**
- **Domain Name System (DNS)**
- **File Transfer Protocol (FTP)**
- **generic routing encapsulation (GRE)**
- Gopher
- HyperText Transport Protocol (HTTP)
- Internet Control Message Protocol (ICMP)

- Internet Protocol (IP)
- NetBIOS over IP (Microsoft Networking)
- Point-to-Point Tunneling Protocol (PPTP)
- Simple Network Management Protocol (SNMP)
- Sitara Networks Protocol (SNP)
- SQL*Net (Oracle client/server protocol)
- Sun Remote Procedure Call (RPC) services, including Network File System (NFS)
- Telnet
- Transmission Control Protocol (TCP)
- Trivial File Transfer Protocol (TFTP)
- User Datagram Protocol (UDP)
- RFC 1700

Reference: Cisco PIX Firewall Software - TCP/IP Reference Information

QUESTION NO: 67
Which type of ACL is allowed when implementing the Cisco IDS IP blocking feature using post-shun ACLs?

A. Numbered IP extended
B. Named IPX extended
C. Numbered IP standard
D. Numbered IPX standard

Answer: A
Explanation: Extended ACLs enable you to create fine-tuned filtering policies.

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 464

QUESTION NO: 68
What reconnaissance methods are used to discover servers running SMTP and SNMP? (Choose two)

A. TCP scans for port 25
B. UDP scans for port 25
C. UDP scans for port 161
D. ICMP sweeps for port 25
E. ICMP sweeps for port 161

Answer: A, C
Explanation:
If the public SMTP server were compromised, a hacker might try to attack the internal mail server over TCP port 25, which is permitted to allow mail transfer between the two hosts. SNMP is a network management protocol that can be used to retrieve information from a network device (commonly referred to as read-only access) or to remotely configure parameters on the device (commonly referred to as read-write access). SNMP agents listen on UDP port 161.

Reference: SAFE Blueprint for Small, Midsize, and Remote-User Networks

QUESTION NO: 69
An attacker has launched an attack against a web server by requesting a web page using the Unicode representation for the slash character in the URL.
What IDS evasive technique is the attacker using?

A. Encryption
B. Fragmentation
C. Flooding
D. Obfuscation
E. Saturation

Answer: D
Explanation: Intrusion detection systems typically implement obfuscation defense - ensuring that suspect packets cannot easily be disguised with UTF and/or hex encoding and bypass the Intrusion Detection systems.

Reference: Cisco Intrusion Detection System - Cisco Security Advisory: Cisco Secure Intrusion Detection System Signature Obfuscation Vulnerability

QUESTION NO: 70
What methods can be used to access the IDSM command line? (Choose two)

A. Telnet
B. Monitor and keyboard
C. IDS Device Manager
D. IDS Event Viewer
E. Session command
F. IDS Management Center

Answer: A, E
Explanation:
The Catalyst 6000 family switch can be accessed either through a console management session or through telnet.

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 498

QUESTION NO: 71
Which Cisco IDS service must be running if a Sensor is capturing network traffic?

A. Managed
B. Captured
C. Snifferd
D. Packetd
E. Traffic d

Answer: D
Explanation:
Packetd - The *packetd* daemon interprets and responds to all of the events it detects on the monitored subnet.

Reference: Cisco Secure IDS Internal Architecture

QUESTION NO: 72
What network devices does Security Monitoring Center monitor? (Choose three)

A. Cisco VPN Concentrators
B. Cisco IDS Sensors
C. Cisco Host IDS software
D. Cisco PIX Firewalls
E. Cisco Catalyst switches
F. Cisco Secure Access Control server

Answer: B, C, D
Explanation: You can use Event Viewer to view real-time and historical events. Events include IDS alerts (generated by network-based and host-based sensors, IOS devices, and PIX devices), syslog messages, and audit logs. This section contains the following topics:

QUESTION NO: 73
What security management product allows IDS Sensor to be grouped for management?

A. CSPM
B. IDS MC
C. IDM
D. IEV

Answer: B
Explanation:
The CiscoWorks Management Center for IDS Sensors is management software for the configuration of network IDS, switch IDS sensors and IDS network modules for routers.
Reference: CiscoWorks Management Center for IDS Sensors

QUESTION NO: 74

What information can a network security administrator specify in a Cisco IDS signature filter? (Choose three)

A. Source port
B. Source address
C. Destination address
D. Destination port
E. Signature ID

Answer: B, C, E
Explanation: A filter is defined by specifying the signature, the source address, and the destination address and whether it is an inclusive or exclusive filter.

Reference: **CiscoWorks Management Center for IDS Sensors - Tuning Sensor Configurations**

QUESTION NO: 75
Match the Signature micro-engine usage description with the micro-engine name.

Detect network reconnaissance	flood
Used for single packet conditions	sweep
Used for character pattern matching	string
Detect attempts to cause denial of service	atomic

Answer:

sweep

atomic

string

flood

Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 628-629

QUESTION NO: 76
Match the description of the terms used when configuring SPAN

Traffic leaving switch port	Ingress filtering
Switch port being monitored	Monitor port
Traffic entering switch port	Egress filtering
Switch port receiving mirrored traffic	Source port

Answer:

Egress filtering	
Source port	
Ingress filtering	
Monitor port	

Explanation:

- Ingress SPAN copies network traffic received by the source ports for analysis at the destination port.
- Egress SPAN copies network traffic transmitted from the source ports for analysis at the destination port.
- A source port is a switch port monitored for network traffic analysis. The traffic through the source ports can be categorized as ingress, egress, or both.
- A destination port (also called a *monitor port*) is a switch port where SPAN sends packets for analysis.

Reference: Cisco Catalyst 6500 Series Switches - Configuring SPAN and RSPAN
QUESTION NO: 77
Enter the Cisco IDB 4210 Sensor command used to initialize the Sensor.

Answer: sysconfig-sensor

Reference: Cisco Intrusion Detection System - Cisco Secure Intrusion Detection Sensor Cabling and Setup Quick Reference Guide

QUESTION NO: 78
Match the Cisco IDS Sensor command with its function.

idsstop	Displays the Cisco IDM service status
cidServer stop	Stops the Cisco IDS services
idsvers	Stops the Cisco IDM service
cidServer version	Displays the Cisco IDS service version

Answer:

Stops the Cisco IDS services
Stops the Cisco IDM service
Displays the Cisco IDS service version
Displays the Cisco IDM service status

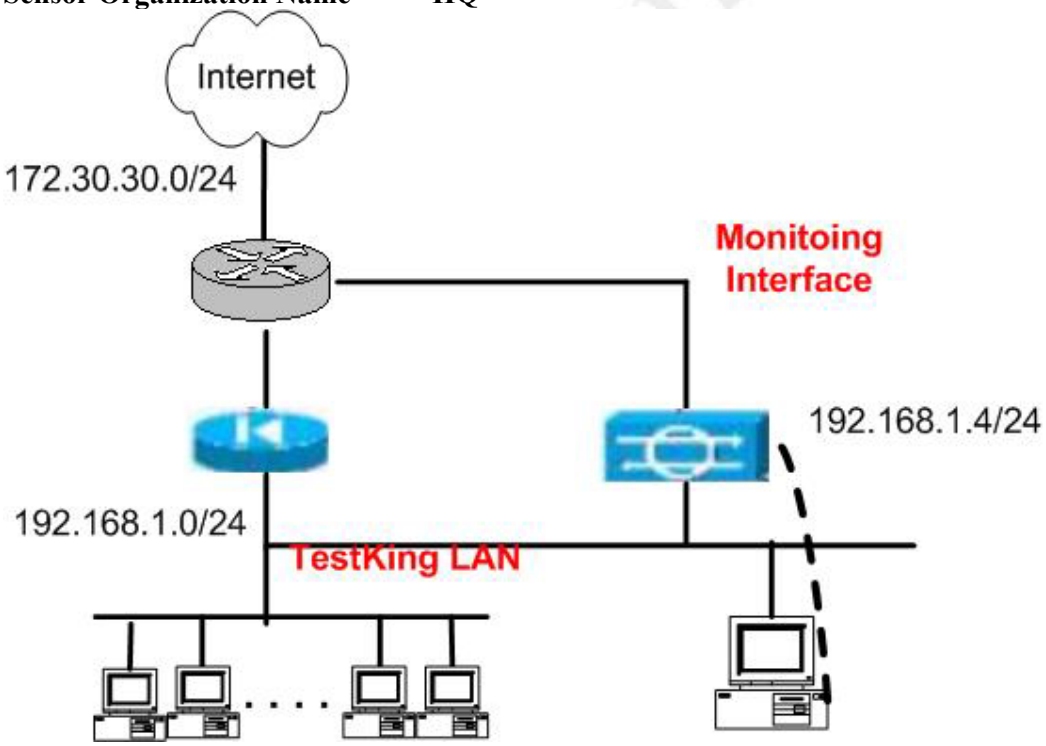
Explanation:
- **idsstop** - Executing this script stops the Cisco IDS daemons.
- **cidServer stop -** If you are troubleshooting an issue with TAC and you need to stop and start the server, enter the following commands

- **idsvers -** To verify the installation of the S10 signature pack, Telnet to the Sensor, log on as **netrangr**, and issue either the **nrvers** or the **idsvers** command.
- **cidServer version –** If you are having difficulty connecting to the sensor via the IDS Device Manager, SSH or Telnet to the sensor and type the **cidServer version** command to check the version and status of the sensor (whether it is running):

Reference: Cisco Secure Intrusion Detection System Internal Architecture
Cisco IDS Sensor Software - Cisco Intrusion Detection System Sensor Getting Started Version 3.1
Updating IDS Appliance Signatures and Troubleshooting Basic Communication

QUESTION NO: 79
TestKing International has decided to deploy a Cisco IDS solution. They have purchased a Cisco IOS 4235 Sensor which has never been configured. You will have to configure and initialize the Sensor to communicate with the Cisco IDS Director using the information listed in the following table:

Cisco IDS Paramaters	**Settings**
Sensor Host ID	**4**
Sensor Organization ID	**27**
Sensor Host Name	**sensor27**
Sensor Organization Name	**HQ**



Assignment: Click on the picture of the host connected to an IDS Sensor by a serial console cable shown in the diagram as a dotted line. Select the Cisco Terminal Option and make the appropriate configuration tasks.

Sensor IP address	**192.168.1.4/24**
IDS Manager Host ID	4

IDS Manager Host Organization ID 27
IDS Manager Host Name sensor 27
IDS Manager Organizaiton Name HQ
IDS Manager IP Address 192.168.1.12/24

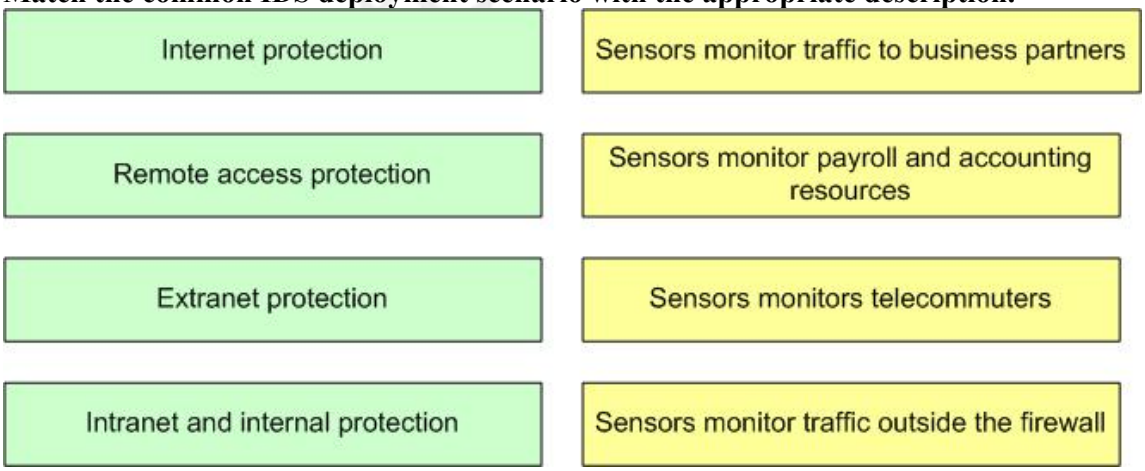
Note: The rout account password is "testking"

Answer:
(Click on the host connected to the IDS Sensor)
Type: sysconfig-sensor
Select option 6 to access the Communications Infrastructure screen, type "y" to enter in the information. Enter information for A, B, C, D, and E
A. Sensor host ID - 4
B. Sensor Organization ID - 27
C. Sensor host name – sensor 27
D. Sensor organization name - HQ
E. Sensor IP address - 192.168.1.4/24
Type "y" to use the IDS Device Manager.

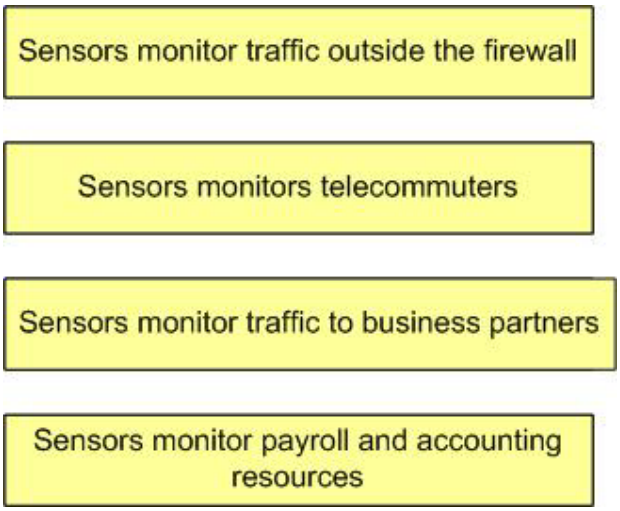
Note: Use the sensor settings, not the director settings.

Reference:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids8/13872_01.htm
Pages 6-12.

QUESTION NO: 80
Match the common IDS deployment scenario with the appropriate description.


Internet protection
Sensors monitor traffic to business partners
Remote access protection
Sensors monitor payroll and accounting resources
Extranet protection
Sensors monitors telecommuters
Intranet and internal protection
Sensors monitor traffic outside the firewall

Answer:


Sensors monitor traffic outside the firewall
Sensors monitors telecommuters
Sensors monitor traffic to business partners
Sensors monitor payroll and accounting resources

Reference: Cisco IOS Intrusion Detection System Software App Overview

www.testking.com

Section B Practice Questions

QUESTION NO: 1
What is a set of rules that pertain to typical intrusion activity?

Answer: signature
Also known as Misuse Detection or Pattern Matching – Matches pattern of malicious activity
Requires creation of signatures
Less prone to false positives-based on the signature's ability to match malicious activity
Cisco Secure Intrusion Detection System 4 chap 3 page 15

QUESTION NO: 2
By default, the event viewer consolidates alarms based on the first two field columns. How do you view the details of collapsed fields?

A. Click Set Current Column.
B. Expand the branch to see your field.
C. Close the event Viewer and reopen it.
D. Click Expand This Branch One Column to the left.

Answer: B

QUESTION NO: 3
What is NSDB?

A. TCP based signatures
B. context buffer data for TCP based signatures.
C. HTML based encyclopedia of network vulnerability information.
D. UDP based exploit signature with information about the signature that triggered the alarm.

Answer: C
The NSDB is the Cisco HTML-based encyclopedia of network vulnerability information.
Cisco Secure Intrusion Detection System 4 chap 10 page 27

QUESTION NO: 4
What is the policy of the Policy server feature set in CSPM?

A. Facilities remote administration of the system.
B. Deletes all the feature sets operating on a single computer.

C. Carries out all database, monitoring, reporting and policy distribution functionality and does not support the management of CSIDS sensors.
D. Stores all system configuration data and summary audit records, generates on-demand or scheduled system reports, compiles global policy down into device specific rules.

Answer: D

QUESTION NO: 5
What happens to the old files when a new configuration file is created?

A. The old file is deleted from the system.
B. The old file is closed and transferred to an archive directory.
C. The old log file remains opened until the administrator deletes it.
D. The old log file remains opened until it has reached 1 GB of data.

Answer: D
By default, log files will be archived and a new one is created when the active log file reaches 1 gb or after 60 minutes have past, which ever comes first
- Cisco Secure Intrusion Detection System 4 chap C page 44

QUESTION NO: 6
What is context based signature?

A. Signature triggered by single packets.
B. Signature triggered by series of multiple packets.
C. Signature triggered by data contained in packet payloads.
D. Signature triggered by data contained in packet headers.

Answer: D
Context based cheking checks for ip header not the data. Content based checking checks for the data.

QUESTION NO: 7
In the 3000 series which TCP signature occurs when one host searched for multiple TCP services on a single host?

A. Mail attack
B. TCP Port scan
C. TCP Host sweep
D. TCP Traffic Record

Answer: B

QUESTION NO: 8
Which utility extracts events recorded from the CSPM database?

A. extract.exe
B. convert.exe
C. cvtnrlog.exe
D. download.exe

Answer: C

QUESTION NO: 9
What is a CSIDS Token?

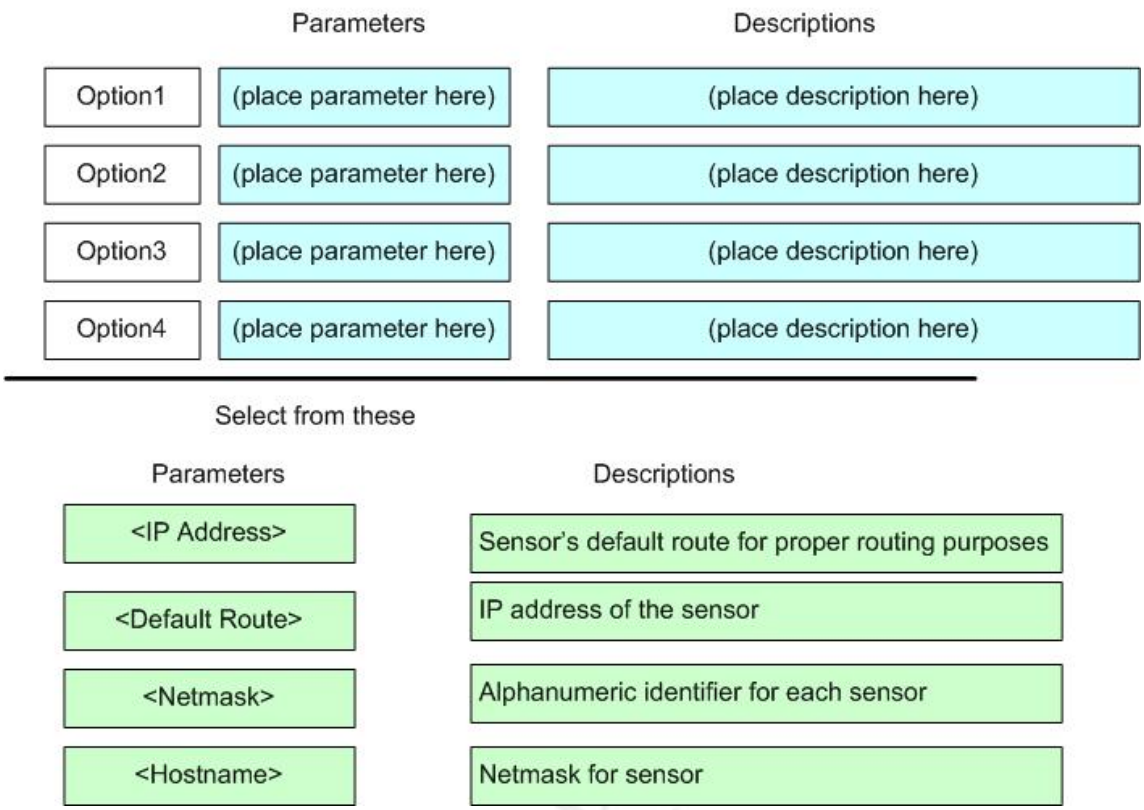
A. Values associated with the CSIDS token.
B. Device name of the monitoring interface on the sensor.
C. Character string identifying a CSIDS service configurable item.
D. Numeric identification of the signature being configured during the session.

Answer: C

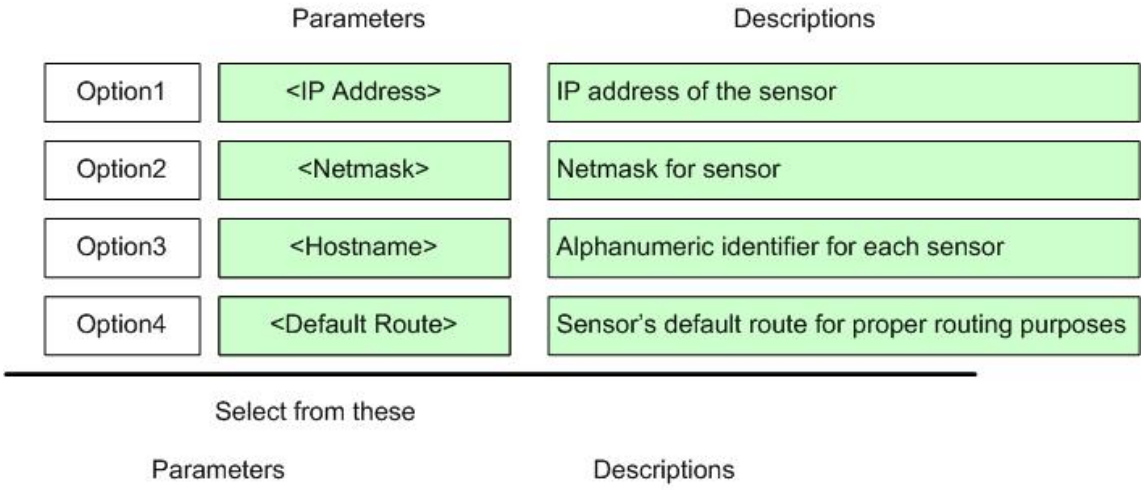
QUESTION NO: 10
Type the command used to commit VLAN ACL's in NVRAM that have not been written to hardware?

Answer: `commit security acl acl_name`

QUESTION NO: 11
During IP configuration on the sensor, there are four options you can use.
Complete the table, showing parameter and description for each option:



Answer:



QUESTION NO: 12
What are ALL the ways to access a sensor to manage it?

A. Connect a monitor and keyboard directly on the sensor use Telnet after the sensor has been assigned an IP address.

B. Access the console port by using an RS-232 cable and a terminal emulation program. Connect a monitor and mouse directly on the sensor.
C. Access the console port by using an RS-232 cable and a terminal emulation program. Use Telnet after the sensor has been assigned an IP address.
D. Access the console port by using an RS-232 cable and a terminal emulation program. Connect a monitor and a mouse directly on the sensor use Telnet after the sensor has been assigned an IP address.
E. Access the console port by using an RS-232 cable and a terminal emulation program. Connect a monitor and a keyboard directly on the sensor use Telnet after the sensor has been assigned an IP address.

Answer: E
Explanation: You HAVE to have a keyboard, you don't have to have a mouse along with the monitor. Ref Cisco Secure Intrusion Detection System p. 149

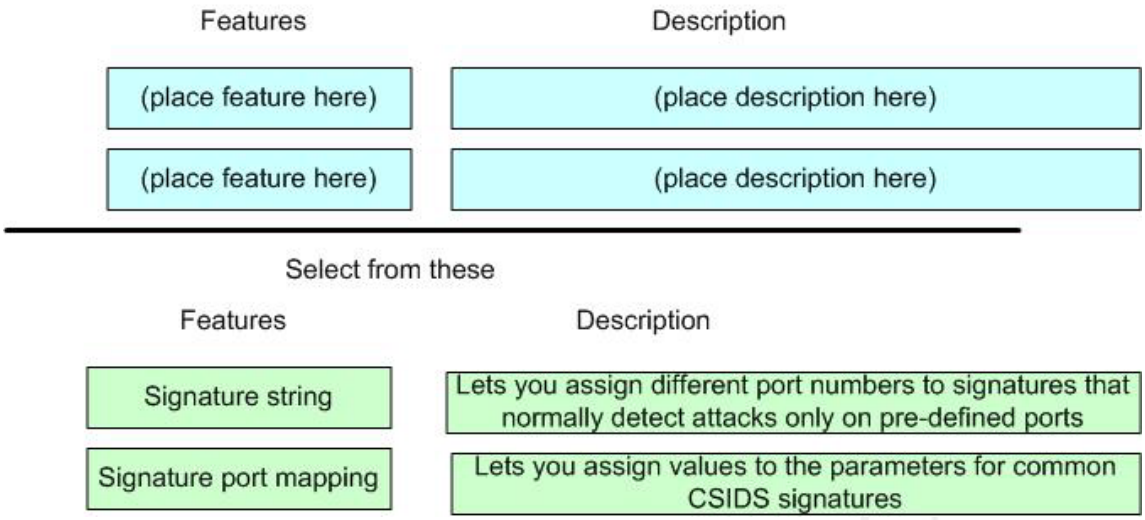
Following are the methods used to gain management access to a Sensor
Console port
Monitor and keyboard
Telnet
SSH
HTTPS
- Cisco Secure Intrusion Detection System 4 chap 7 page 23

QUESTION NO: 13
When applying ACL's on the external interface, what is true?

A. The host is denied before it enters the router.
The shun does not apply to the router itself.
The user-defined ACL's are applied to the external interface.
B. The host is denied before it enters the router.
It provides the best protection against an attacker.
The user-defined ACL's are applied to the internal interface.
C. The host is denied before it enters the protected network.
The shun does not apply to the router itself.
The user-defined ACL's are applied to the external interface.
D. The host is denied before it enters the protected network.
The best protection against an attack is provided.
The user-defined ACL's are applied to the external interface.

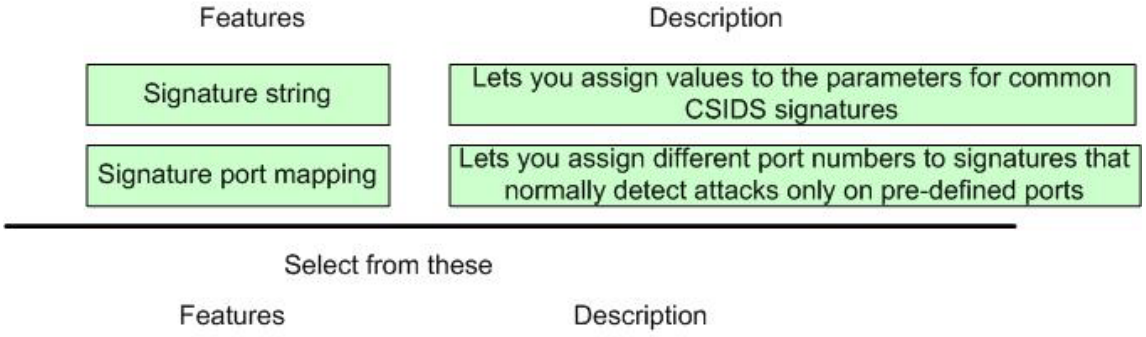
Answer: B

QUESTION NO: 14
Match features with the appropriate descriptions.'

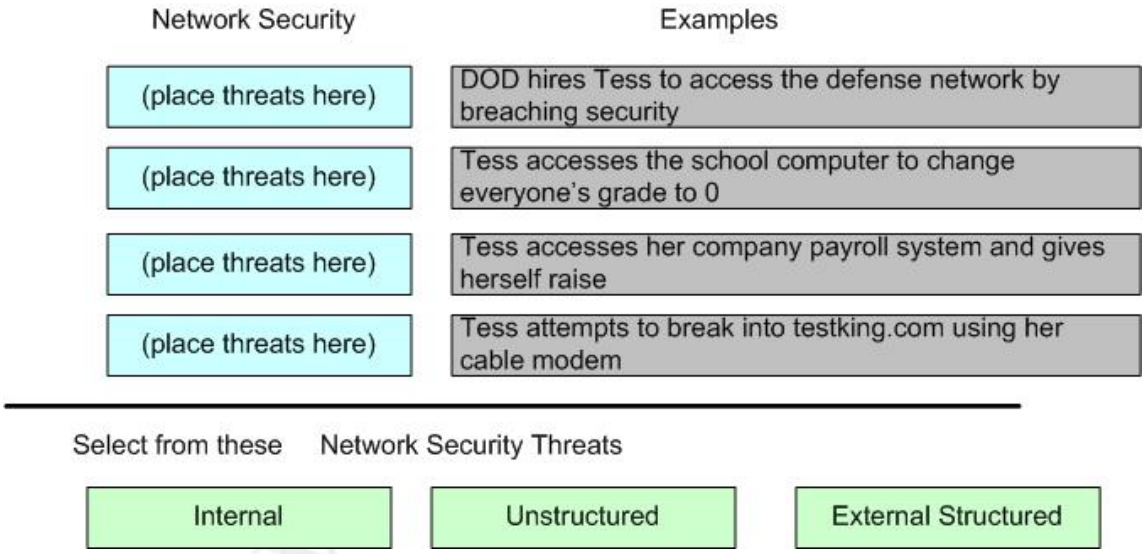


www.testking.com

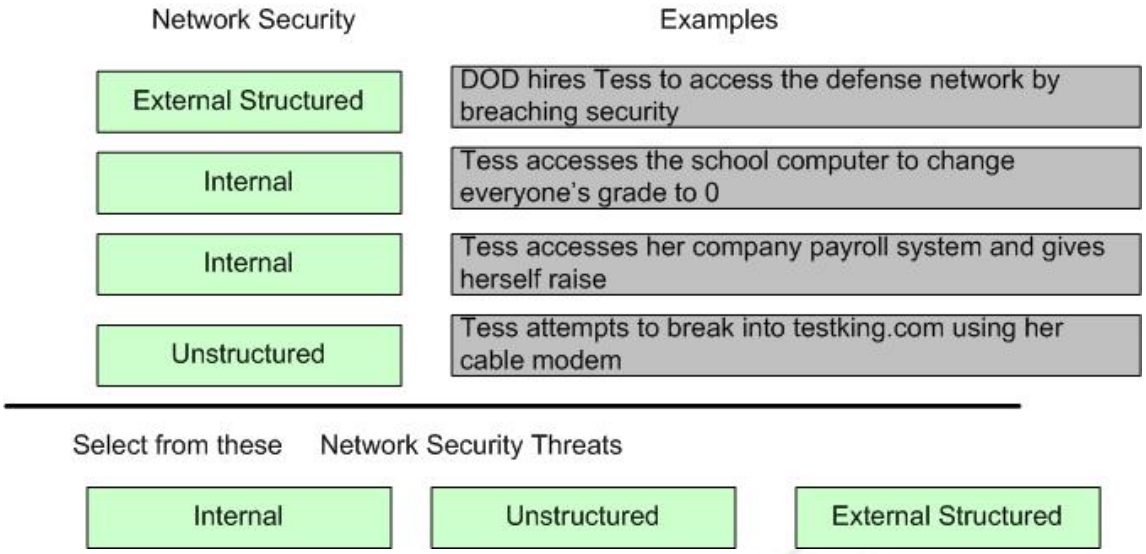
Answer:


Features
Description
Signature string
Lets you assign values to the parameters for common CSIDS signatures
Signature port mapping
Lets you assign different port numbers to signatures that normally detect attacks only on pre-defined ports
Select from these
Features
Description

QUESTION NO: 15
Place each network security threat next to its example:


Network Security
Examples
(place threats here)
DOD hires Tess to access the defense network by breaching security
(place threats here)
Tess accesses the school computer to change everyone's grade to 0
(place threats here)
Tess accesses her company payroll system and gives herself raise
(place threats here)
Tess attempts to break into testking.com using her cable modem
Select from these
Network Security Threats
Internal
Unstructured
External Structured

Answer:


Network Security
Examples
External Structured
DOD hires Tess to access the defense network by breaching security
Internal
Tess accesses the school computer to change everyone's grade to 0
Internal
Tess accesses her company payroll system and gives herself raise
Unstructured
Tess attempts to break into testking.com using her cable modem
Select from these
Network Security Threats
Internal
Unstructured
External Structured

QUESTION NO: 16
Which command used to determine the CSIDS service status?

Answer: `nrstatus`

QUESTION NO: 17
What are three functions of sensor? (Choose three)

A. Logs and display alarms.
B. Configures display alarms.
C. Impacts switch performance.
D. Detects unauthorized activity.
E. Responds to authorized activity.
F. Responds only to authorized activity.
G. Reports unauthorized activity to a sensor platform.
H. Reports unauthorized activity to a Director platform.

Answer: A, D, H

QUESTION NO: 18
How do you get information on the status of the connection between CSPM and the sensors reporting to it while on the connection status pane?

A. Left click the correct sensor on the connection status Pane and choose Service Status.

B. Right click the correct sensor on the connection status Pane and choose Service Status.
C. Left click the correct sensor on the connection status Pane and choose Connection Status.
D. Right click the correct sensor on the connection status Pane and choose Connection Status.

Answer: D

QUESTION NO: 19
Within the policy database server group, which option is used for login with a standalone installation?

A. Local server
B. Client server
C. Remote server
D. Director

Answer: A

QUESTION NO: 20
Which two signatures are considered to be HTTP signatures? (Choose two)

A. WWW UDP Bomb
B. WWW Inn Control Message
C. WWW UDP Traffic Records
D. WWW IIS Virtualized UNC Bug
E. WWW IIS Showcode .asp Access
F. WWW IOS Command History Exploit

Answer: D, E

QUESTION NO: 21
Which statement describes ICMP Smurf attack?

A. A large number of ICMP Echo Replies is targeted as a machine.
B. A small number of ICMP Echo Replies is targeted as a machine.
C. An IP datagram is received with the protocol field of the IP head set to 1.
D. A large number of ICMP source Quench requests is targeted at a machine.
E. Multiple IP datagrams are received that are directed at a single host on the network.

F. An ICMP datagram is received with the protocol field of the ICMP header set to 1 and either the more fragments flag is set to 1 or there is an offset indicated in the offset field.

Answer: A

QUESTION NO: 22
What is an ACL Token?

A. SifOfTcpPacket
B. SigOfUdpPacket
C. RecordOfFilterName
D. RecordOfStringName

Answer: C
RecordOfFilterNames <sub-signature><acl_name|acl_number> - defines cisco ids acl signatures settings
- Cisco Secure Intrusion Detection System 4 chap C page 30

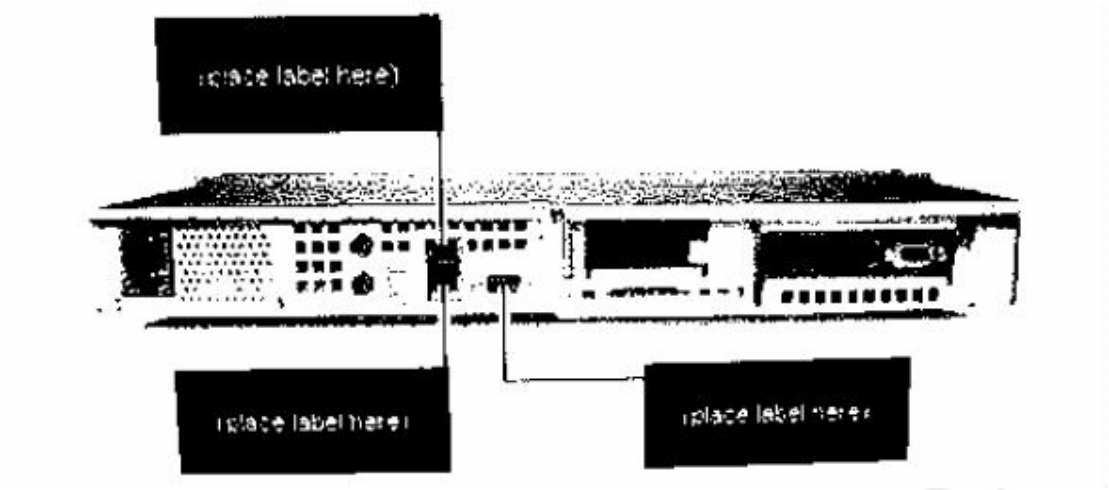
QUESTION NO: 23
The CSIDS configuration files, what does the organization file contain?

A. Organization ID and WatchDogInterval.
B. Organization ID and Organization name.
C. Organization ID and TimeOutAlarmLevel.
D. Organization name and WatchDogInterval.

Answer: B

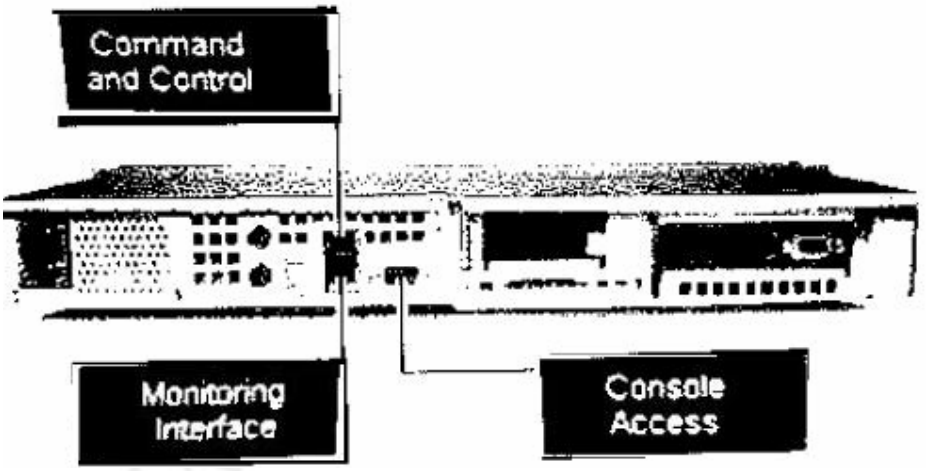
QUESTION NO: 24
Drag and drop, label the back panel of the 4210 sensor:

www.testking.com



Labels to me moved:

Answer:



Reference: Cisco Secure Intrusion Detection System p. 166-168
Cisco Secure Intrusion Detection System 4 chap 7 page 5

QUESTION NO: 25
How do you push a signature template to a sensor in CSPM?

A. Select the sensor from the NTT, select the command tab in the sensor view panel.
B. Select the control tab in the sensor view panel, click the APPROVE NOW button in the command approval section.
C. Select the sensor from the NTT, select the Control tab, click the approve Now button in the command approval section.

D. Select the sensor from the NTT, select the command tab in the sensor view panel, click the approve Now button in the command approval section.

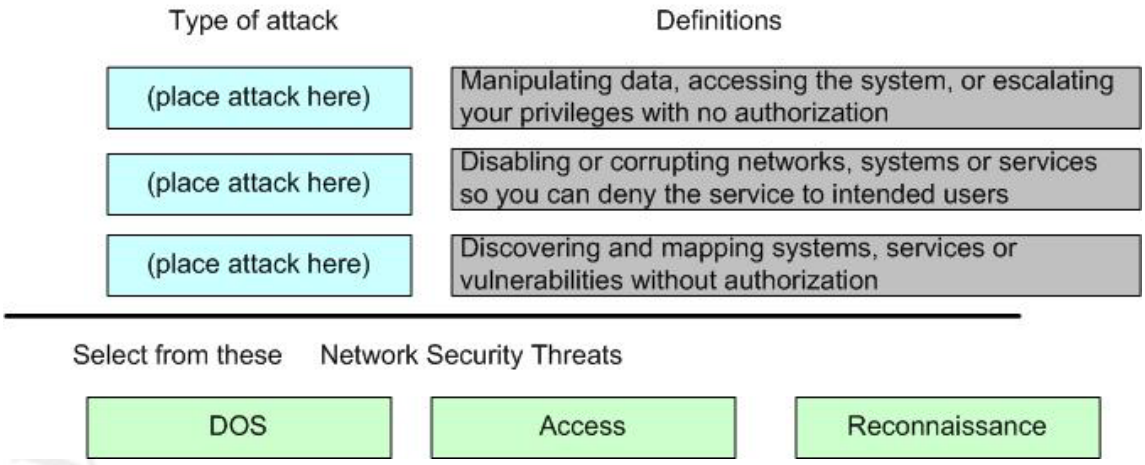
Answer: D

QUESTION NO: 26
Which steps are necessary to create ACL signatures?

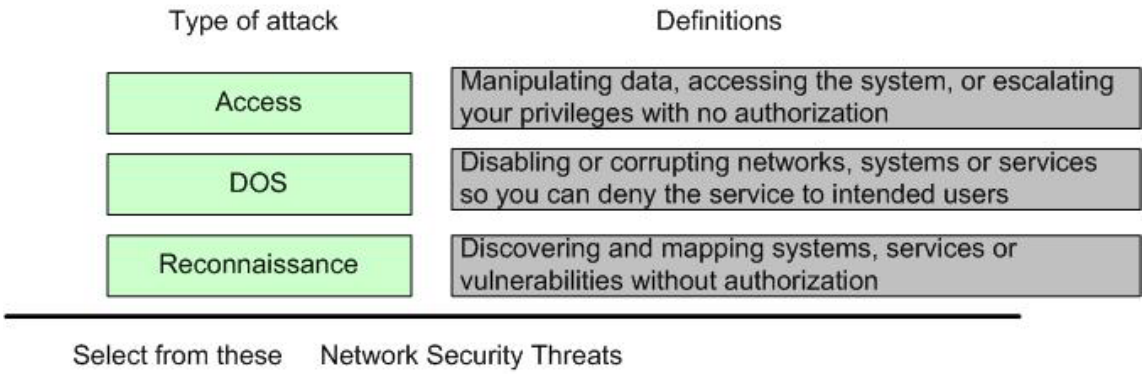
A. Create the ACL to monitor and select the signature template.
B. Create a new ACL and configure the director to monitor syslog messages from the network device.
C. Create the ACL to monitor and configure the sensor to monitor syslog messages from the network device.
D. Select the signature template and configure the sensor to monitor config messages from the network device.

Answer: C

QUESTION NO: 27
Drag and drop:


Type of attack
Definitions
(place attack here)
Manipulating data, accessing the system, or escalating your privileges with no authorization
(place attack here)
Disabling or corrupting networks, systems or services so you can deny the service to intended users
(place attack here)
Discovering and mapping systems, services or vulnerabilities without authorization
Select from these
Network Security Threats
DOS
Access
Reconnaissance

Answer:


Type of attack
Definitions
Access
Manipulating data, accessing the system, or escalating your privileges with no authorization
DOS
Disabling or corrupting networks, systems or services so you can deny the service to intended users
Reconnaissance
Discovering and mapping systems, services or vulnerabilities without authorization
Select from these
Network Security Threats

QUESTION NO: 28
Which command removes configuration information on the IDSM?

Answer: `clear config`

QUESTION NO: 29
What does the alarm context buffer contain?

A. Data only
B. Keystrokes only
C. Keystrokes, data or both
D. Neither keystrokes nor data

Answer: C

QUESTION NO: 30
What is the Hostname on the PostOffice settings?

A. Numeric identifier for CSPM.
B. IP address of the CSPM host.
C. Alpha identifier that further identifies CSPM.
D. Alphanumeric identifier for CSIDS component.

Answer: D

Hostname – an alphanumeric identifier for the cisco ids device. The name chosen here is typically one that describes the name and location where the device is installed (senor1_austin)
Cisco Secure Intrusion Detection System 4 chap C page 8

QUESTION NO: 31
Which RPC attack signature determines the presence and port location of RPC services being provided by a system?

A. RPC dump
B. Proxied RPC request
C. RPC port registration
D. RPC port unregistration

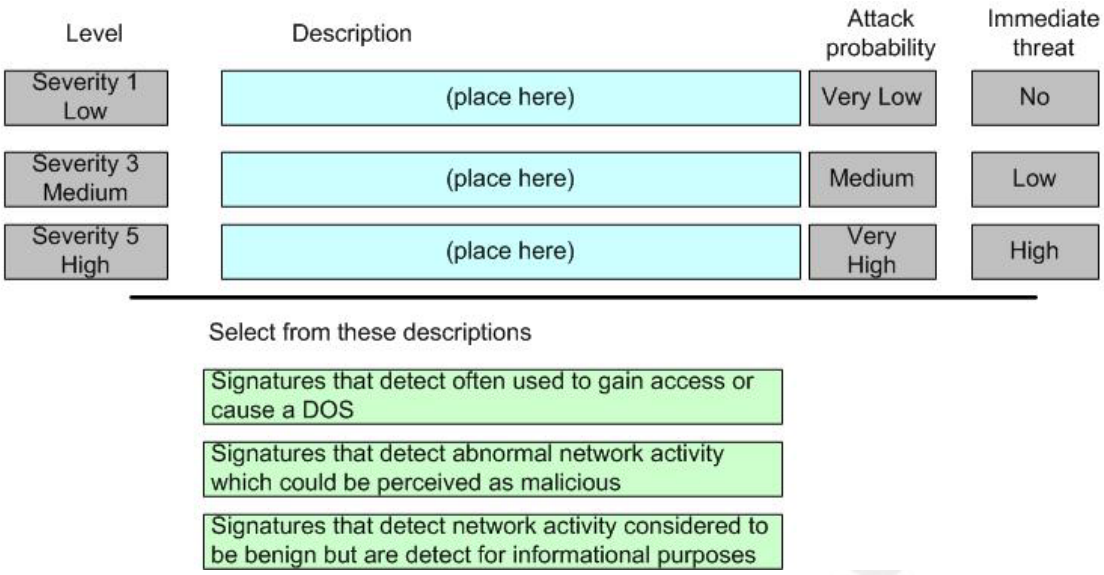
Answer: A

QUESTION NO: 32
What is the function of CSIDS application file?

A. They define CSIDS application identification and associated service names.
B. They allow you to add additional destinations to send events generated by CSIDS.
C. They enable you to set which CSIDS services are started every time CSIDS is launched.
D. They enable you to set appropriate permissions for other CSIDS components to remotely query and configure the current CSIDS component, sensor or director.

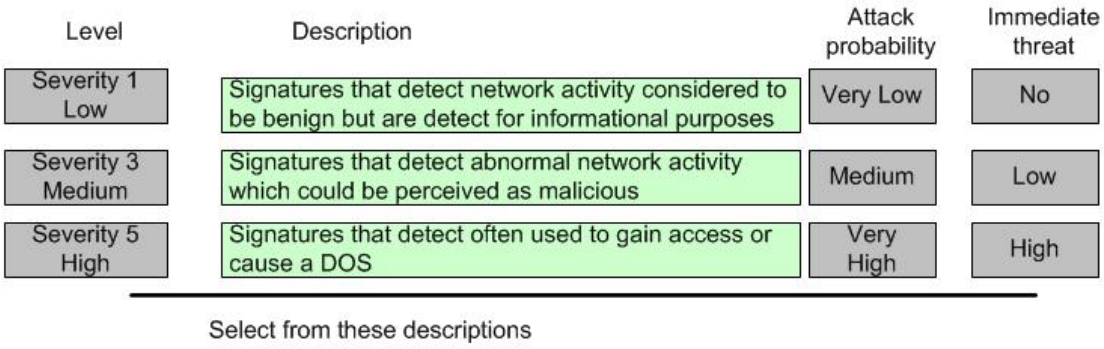
Answer: A
Cisco IDS applications
<application id> <service name> - maps cisco ids applications identification and associated service names
- Cisco Secure Intrusion Detection System 4 chap C page 58

QUESTION NO: 33
Drag and drop, match the description of signature severity to the severity level, attack probability, and the immediate threat risk:



www.testking.com

Answer:



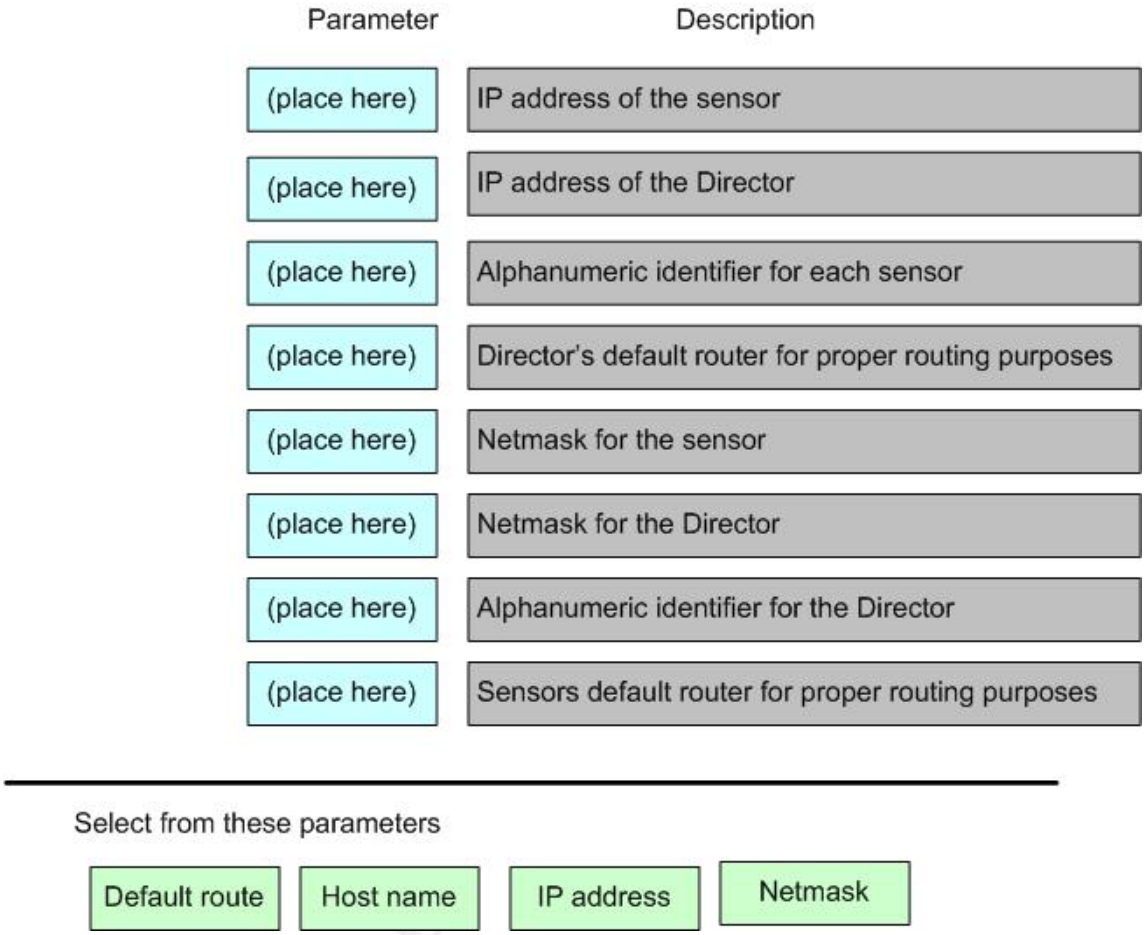
QUESTION NO: 34
Which partition of the IDSM components is active by default?

A. boot
B. signatures
C. application
D. maintenance

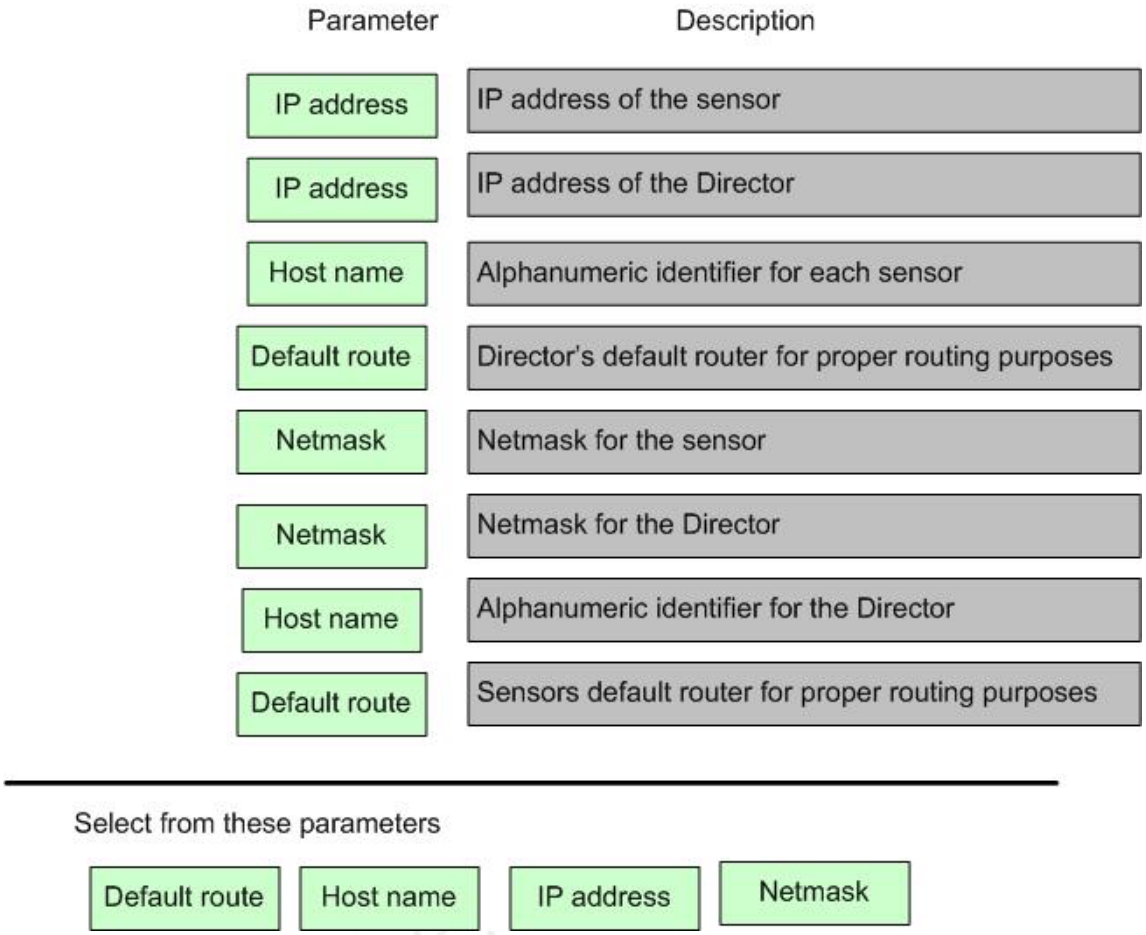
Answer: C

www.testking.com

QUESTION NO: 35
Drag and drop.
Move the parameters to the appropriate places.



Answer:



QUESTION NO: 36
What must you do first to identify an inside our outside network address?

A. Select a signature.
B. Define an internal network.
C. Define an external network.
D. Select a signature with a pre-defined sub-signature.

Answer: B

QUESTION NO: 37
Which command displays the module status and information?

Answer: `show module`

QUESTION NO: 38
In preference settings for the Event viewer, which statement about the Blank left checkbox is true?

A. When it is selected, the actual value is displayed.
B. When it is not selected, the actual value is displayed.
C. When cells are collapsed, the background color is gray.
D. If the collapse values are different, a "+" sign is displayed.

Answer: B

QUESTION NO: 39
Which statement about a loose TCP session reassembly is true?

A. The sensor immediately processes all packets in a stream.
B. The sensor is configured to track only those sessions for which the three-way handshake is completed.
C. The sensor does not process TCP sessions for which it cannot track every packet in the session's sequence.
D. The sensor permits sequence gaps when it attempts to reassemble all packets into a composite session record.

Answer: D

QUESTION NO: 40
When using the ICMP signatures in the 2000 series, what are the Ping Sweep signatures?

A. ICMP Smurf sweep, ICMP Ping of Death.
B. Fragmented ICMP sweet, Large ICMP sweep, ICMP Flood.
C. Unreachable Sweep, Source quench sweep, Redirect sweep, Time exceeded sweep.
D. ICMP network sweep with Echo, ICMP network sweep with Timestamp, ICMP network sweep with address mask.

Answer: D

QUESTION NO: 41
What is the organization name for the PostOffice?

A. Numeric identification for the CSIDS host.
B. Numeric identification for the CSIDS organization.
C. Alphanumeric identifier for a group of CSIDS devices.
D. Combination of host identification and organization identification.

Answer: C
The organization name is an Alphanumeric identifier for a group of CSIDS devices.

QUESTION NO: 42
What is the catalyst 6000 IDSM?

A. A product that enables sensors to propagate messages to up to 255 destinations.
B. A Sensor, Director and PostOffice each with a separate operational software component.
C. A switch line card designed to address switched environments by integrating IDS functionality directly into the router.
D. A switch line card designed to address switched environments by integrating IDS functionality directly into the switch.
E. The Director platform of the CSIDS management system that includes alarm management, remote sensor configuration, event processing and database functions.

Answer: D

QUESTION NO: 43
How do you defend a network using the Cisco IOS router for blocking?

A. Examine size and complexity.
Examine connections between your network and other networks.
Examine amount and type of network traffic.
B. Enable Telnet services on the router add the router to the sensors device management list ensure the sensor has access to the management router.
C. Enable Telnet services on the router add the router to the sensors device management list.
Configure the firewall to allow for traffic that travels via Telnet from the sensors monitoring interface to the router.
D. Enable Telnet services on the router form the sensor add the router to the Directors device management list configure the firewall to allow Telnet traffic from the sensors command and control interface to the router and UDP port 45000 traffic through the firewall and the routers to the director.
Configure the routers for IPSec encryption.

Answer: C

QUESTION NO: 44
What should you do to disable signatures from the CSPM?

A. Select the Enable checkbox.
B. Select the disable checkbox.
C. Deselect the Enable checkbox.
D. Deselect the disable checkbox.

Answer: C

QUESTION NO: 45
What do you set Propagate Most Critical in HP Openview's Network Node Management user interface?

A. To enable the CSIDS UNIX Director to propagate the most severe alarms to a secondary Director.
B. To allow the color associated with the most server alarm icon to be propagated through all submaps.
C. To enable the CSIDS UNIX Director to propagate the most server alarms to the Cisco router for shunning.
D. To allow the color associated with the most severe alarm icon to be propagated up the next sub map level only.

Answer: B

QUESTION NO: 46
Which statement about the command Timeout in the Event Viewer's Preference settings is true?

A. It is published to the blocking devices by the sensor.
B. It is the length of time CSPM waits for a response from a Sensor.
C. Ip applies only to blocks that are generated automatically by that sensor.
D. It is the length of time a sensor blocks a host when a manual block is issued.

Answer: B

QUESTION NO: 47
What is a atomic signature?

A. Signature triggered by single packets.

B. Signature triggered by series of multiple packets.
C. Signature triggered by data contained in packet payloads.
D. Signature triggered by data contained in packet headers.

Answer: A

QUESTION NO: 48
Which CSIDS software service is responsible for capturing network traffic and performing intrusion detection analysis?

A. nr.packetd
B. nr.managed
C. packetd.conf
D. SigOfGeneral

Answer: A

QUESTION NO: 49
What tab is used to define a sensor that will perform IP blocking in its behalf?

A. Sensing
B. Advanced
C. Super blocking sensor
D. Master blocking sensor
E. Master blocking director

Answer: D

QUESTION NO: 50
Which four security solutions should be implemented to secure the network when using the Cisco Security? (Choose four)

A. Firewalls
B. Trojan horses
C. Authentication
D. Security holes
E. Resource packets
F. Vulnerability patching
G. Virtual private network

Answer: A, C, F, G
Implement security solutions to stop or prevent unauthorized access or activities, and protect information – authentication – encryption – firewalls – vulnerability patching
- Cisco Secure Intrusion Detection System 4 chap 2 page 14

QUESTION NO: 51
Which statement about the creation of different signature template is TRUE?

A. You can change settings, and then revert to a previous version.
B. You can change settings, but you cannot revert a previous version.
C. It is impossible to maintain multiple version of the signature settings.
D. You can experiment with different settings, but you must re-create the signature-template.

Answer: A

QUESTION NO: 52
What do you define internal networks within CSIDS?

A. To add internal network definitions.
B. To add external network definitions.
C. To allow CSPM to associate alarm locations as IN and OUT.
D. To log all alarm outside (OUT) to outside (OUT) attacks.

Answer: C

QUESTION NO: 53
What are the purposes of the ports on the catalyst 6000 IDSM?

A. Port 1 is a trunking port, port 2 is assigned as the destination capture for VLAN ACL's.
B. Port 1 is for monitoring the network for attacks, Port 2 is the command and control port for the communicating with the Directors software.
C. Port 1 is the command and control port for communicating with the Director Software, Port 2 is for monitoring the network attacks.
D. Port 1 is assigned an IP address during the initial IDSm setup, Port 2 is assigned as the destination capture for VLAN ACL's and is a trunking port.

Answer: B
Understand that in ealier revision of the course that the answer above maybe correct, however as of version 4 this answer would not be correct.

The IDSM2 has the following four logical ports
Port 1 –tcp reset
Port 2 – Command and control
Port 7 or 8 Monitoring
- Cisco Secure Intrusion Detection System 4 chap 17 page 10

QUESTION NO: 54
Why should you consider network entry points when designing IP blocking?

A. They prevent all denial of attacks.
B. They are considered critical hosts and should not be blocked.
C. They provide different avenues for the attacker to attack your network.
D. They provide a method for the sensor to route through the subnet to the managed router.

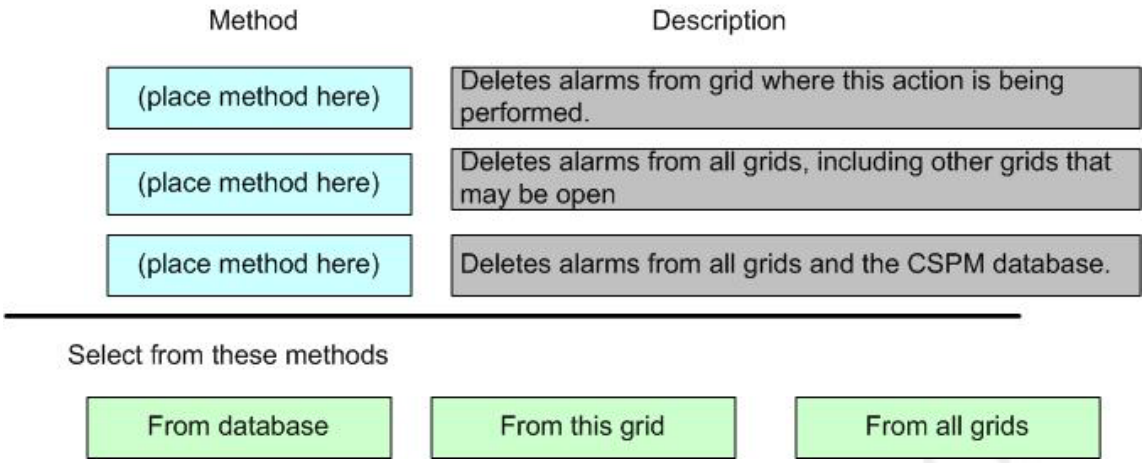
Answer: C
It is recommended that Sensors be placed at those network entry and exit points that provide sufficient intrusion detection coverage. Cisco Secure Intrusion Detection System 4 chap 4 page 37

QUESTION NO: 55
In the sensing tab, which pull down menu assigns signature templates to a sensor?

A. set span disable
B. set security acl ip
C. acl configuration default
D. active configuration default

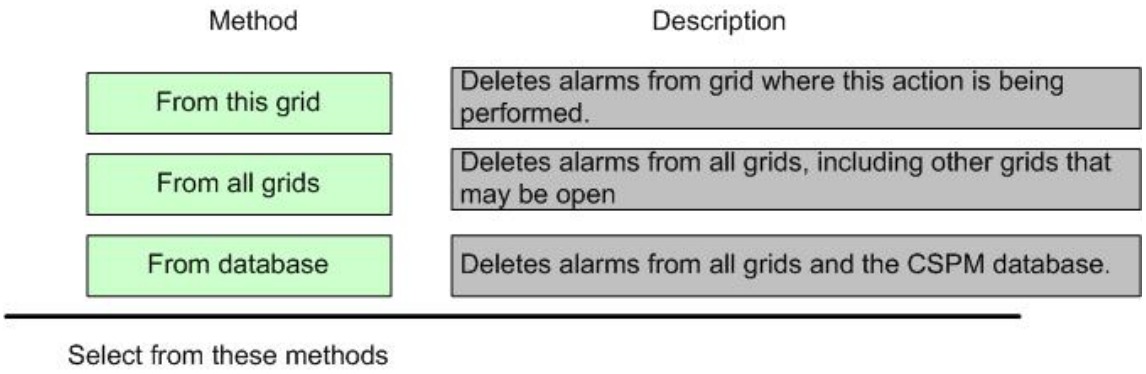
Answer: D

QUESTION NO: 56
Place the methods for deleting alarms next to the descriptions:


Method
Description
(place method here)
Deletes alarms from grid where this action is being performed.
(place method here)
Deletes alarms from all grids, including other grids that may be open
(place method here)
Deletes alarms from all grids and the CSPM database.
Select from these methods
From database
From this grid
From all grids

www.testking.com

Answer:


Method
Description
From this grid
Deletes alarms from grid where this action is being performed.
From all grids
Deletes alarms from all grids, including other grids that may be open
From database
Deletes alarms from all grids and the CSPM database.
Select from these methods

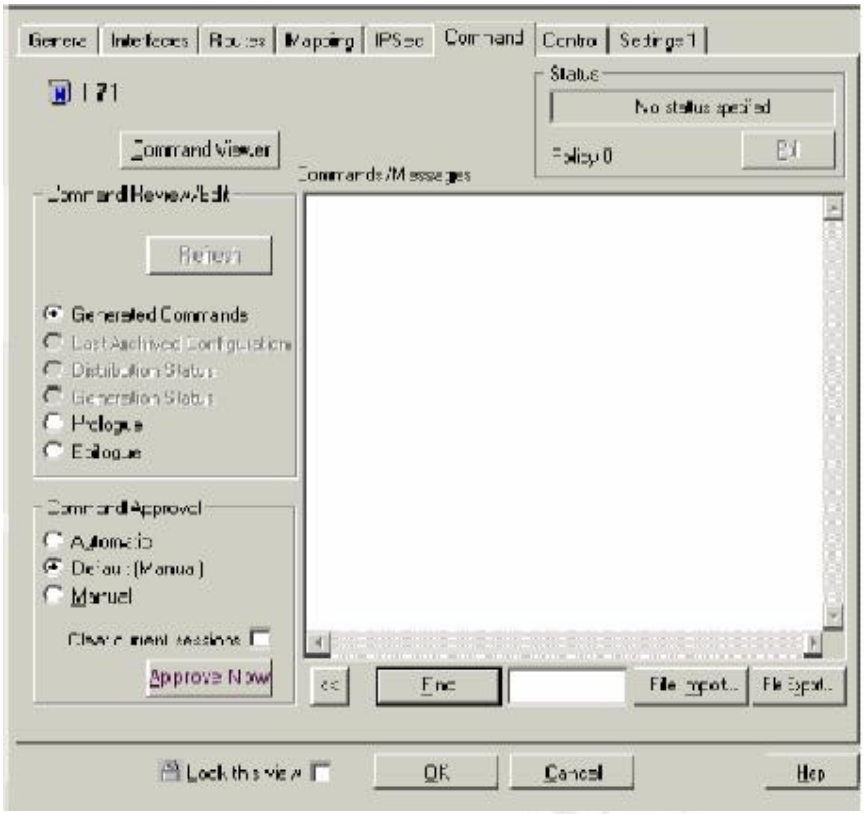
QUESTION NO: 57
What is the most complete list of DDos attack signatures?

A. TFTP, Stacheldraht, mstream
B. TFN, Stacheldraht, Trinoo, TFN2K, mstream
C. statd, ttdb, mountd, cmsd, sadmind, amd, rexd
D. TFN, Trinoo, TFN2K, mstream, statd, sadmind, amd

Answer: B

QUESTION NO: 58
Click the button that generates the configuration files that can be pushed to the sensor:

www.testking.com



Answer:
Explanation: The correct answer isn't available because you need more of the screen shot. In order to CREATE the files to push to the sensor, you click the update button on main GUI toolbar, but we can't see this on the screen shot. To actually send the config files to the sensor, you click on Apply Now.

Reference: Cisco Secure Intrustion Detection System p. 166-168

QUESTION NO: 59
When configuring the sensor to send alarms to additional destinations, which services can receive alarms?

A. smid, eventd, loggerd
B. eventd, loggerd, sapd
C. directord, eventd, smid
D. smid, loggerd, directord

Answer: A

Note : Section A contains 80 questions. Section B contains 59 questions. The total number of questions is 139.